ANALYSIS OF THE WIDTH-w NON-ADJACENT FORM IN CONJUNCTION WITH HYPERELLIPTIC CURVE CRYPTOGRAPHY AND WITH LATTICES

DANIEL KRENN

ABSTRACT. We analyse the number of occurrences of a fixed non-zero digit in the width-w non-adjacent forms of all elements of a lattice in some region (e.g. a ball). Our result is an asymptotic formula, where its main term coincides with the full block length analysis. In its second order term a periodic fluctuation is exhibited. The proof follows Delange's method. This result in a general lattice set-up is then used for numeral systems with an algebraic integer as base. Those come from efficient scalar multiplication methods (Frobenius-and-add methods) in hyperelliptic curves cryptography, and our result is needed for analysing the running time of such algorithms.

1. INTRODUCTION

One main operation in hyperelliptic curve cryptography is building (large) multiples of an element of the Jacobian variety of a hyperelliptic curve over a finite field. Clearly, we want to perform that scalar multiplication as efficiently as possible. A standard method there are double-and-add algorithms, where the multiple to build is written in binary, and then a Horner scheme is performed. By using windowing methods that algorithms can be sped up. The idea is to take a larger digit set and choose an expansion which has a low number of non-zero digits. This leads to an efficient evaluation. Some background information on hyperelliptic curve cryptography can be found for example in [1].

If the hyperelliptic curve is defined over a finite field with q elements and we are working over an extension (over a field with q^m elements), then one can use a Frobenius-and-add method instead. There the (expensive) doublings are replaced by the (cheap) evaluation of the Frobenius endomorphism on the Jacobian variety: If

$$z = \sum_{\ell=0}^{L-1} \xi_\ell \tau^\ell$$

with digits ξ_ℓ and where the base τ is a zero of the characteristic polynomial of the Frobenius endomorphism on the Jacobian, then for an element Q of the Jacobian we can compute zQ by

$$zQ = \sum_{\ell=0}^{L-1} \xi_\ell \, \varphi^\ell(Q) \,,$$

where φ denotes the Frobenius endomorphism. That base τ is an algebraic integer whose conjugates all have the same absolute value, cf. Deligne [7], Dwork [8] and Weil [19, 20, 21], and see Section 11 for more details.

So let us consider digital expansions with a base as above. Let w be a positive integer. Our digit set should consist of 0 and one representative of every residue class modulo τ^w which is not divisible by τ. That choice of the digit set yields redundancy, i.e., each element of $\mathbb{Z}[\tau]$ has more than one representation. The width-w non-adjacent form, w-NAF for short, is a special representation: Every block of w consecutive digits contains at most one non-zero digit. The choice of the digit set guarantees that the w-NAF-expansion is unique. The low weight (number of non-zero digits) of that expansion makes the arithmetic on the hyperelliptic curves efficient.

In the case that the base τ is an imaginary-quadratic algebraic integer properties of such w-NAF numeral systems are known: The question whether for a given digit set each element of $\mathbb{Z}[\tau]$ has a representation as a w-NAF is investigated in Koblitz [16], Solinas [17, 18], Blake, Murty and Xu [3, 5, 4], and Heuberger and Krenn [12]. Another question, namely whether the w-NAF is an expansion which minimises the weight among all possible expansions with the same digit set, is answered in Heuberger and Krenn [13]. A generalisation of those existence and optimality results to higher degree of the base τ is given in Heuberger and Krenn [14]. One main step there was to use Minkowski map to transform the τ-adic setting to a lattice, see also Section 11.

The present work deals with analysing the number of occurrences of a digit in w-NAF-expansions with base τ (an algebraic integer of degree n). This is needed for the analysis of the running time of the scalar multiplication algorithm mentioned at the beginning of this introduction. As brought up in the previous paragraph, we will do this analysis in the set-up of numeral systems in lattices, cf. Section 11. Our main result is the asymptotic formula

$$Z_\eta = N^n \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)} E \log N + N^n \, \psi_\eta(\log N) + \mathcal{O}\left(N^\beta \log N\right).$$

for the number of occurrences of a fixed non-zero digit η in w-NAF-expansions in a ball around 0 with radius N. The main term of that formula coincides with the full block length analysis given in Heuberger and Krenn [12]. There an explicit expression for the expectation (the constant E) and the variance of the occurrence of such a digit in all expansions of a fixed length is given. The result here is more precise: A periodic fluctuation ψ_η in the second order term is also exhibited. The third term is an error term with $\beta < n$. Such structures—main term, oscillation term, smaller error term—are not uncommon in the context of digits counting, see for instance, Heuberger and Prodinger [15] or Grabner, Heuberger and Prodinger [10]. The result itself is a generalisation of the one found in Heuberger and Krenn [12]. The proof, as the one in [12], follows Delange's method, cf. Delange [6], but several technical problems have to be taken into account.

The structure of this article is as follows. We start with the formal definition of numeral systems and the non-adjacent form in Section 2. Sections 3 and 4 contain our primary set-up in a lattice. We will work in this set-up throughout the entire article. There also the used digit set, which comes from a tiling by the lattice, is defined. Additionally, some notations are fixed and some basic properties are given. The end of Section 3 is devoted to the full block length analysis theorem given in Heuberger and Krenn [12]. In Sections 5 to 9 a lot of properties of the investigated expansions, such as bounds of the value and the behaviour of the fundamental domain and the characteristic sets, are derived. Those are needed to prove our main result, the counting theorem in Section 10. The last section will

forge a bridge to the τ-adic set-up. This is explained with details there and the counting theorem is restated in that set-up.

A last remark on the proofs given in this article. As this work is a generalisation of Heuberger and Krenn [12] several proofs of propositions and lemmata are skipped. All those are straight forward generalisations of the ones for the quadratic case, which means, we have to do things like replacing $\mathbb{Z}[\tau]$ by the lattice, the multiplication by τ by a lattice endomorphism, the dimension 2 by n, using a norm instead of the absolute value, and so on. If the generalisation is not that obvious, the proofs are given.

2. Non-Adjacent Forms

This section is devoted to the formal introduction of width-w non-adjacent forms. Let Λ be an Abelian group, Φ an injective endomorphism of Λ and w a positive integer. Later, starting with the next section, the group Λ will be a lattice with the usual addition of lattice points.

We start with the definition of the digit set used throughout this article.

Definition 2.1 (Reduced Residue Digit Set). Let $\mathcal{D} \subseteq \Lambda$. The set $\mathcal{D}$ is called a *reduced residue digit set modulo* Φ^w, if it is consists of 0 and exactly one representative for each residue class of Λ modulo $\Phi^w \Lambda$ that is not contained in $\Phi\Lambda$.

Next we define the syntactic condition of our expansions. This syntax is used to get unique expansions, because our numeral systems are redundant.

Definition 2.2 (Width-w Non-Adjacent Forms). Let $\boldsymbol{\eta} = (\eta_j)_{j \in \mathbb{Z}} \in \mathcal{D}^{\mathbb{Z}}$. The sequence $\boldsymbol{\eta}$ is called a *width-w non-adjacent form*, or *w-NAF* for short, if each factor $\eta_{j+w-1} \ldots \eta_j$, i.e., each block of width w, contains at most one non-zero digit.

Let $J := \{j \in \mathbb{Z} : \eta_j \neq 0\}$. We call $\sup(\{0\} \cup (J + 1))$ the *left-length of the w-NAF $\boldsymbol{\eta}$* and $-\inf(\{0\} \cup J)$ the *right-length of the w-NAF $\boldsymbol{\eta}$*. Let ℓ and r be elements of $\mathbb{N}_0 \cup \{\mathsf{fin}, \infty\}$, where fin means finite. We denote the *set of all w-NAFs of left-length at most ℓ and right-length at most r* by $\mathbf{NAF}_w^{\ell.r}$. The elements of the set $\mathbf{NAF}_w^{\mathsf{fin}.0}$ will be called *integer w-NAFs*. The *most-significant digit* of a $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ is the digit $\eta_j \neq 0$, where j is chosen maximally with that property.

For $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ we call

$$\mathsf{value}(\boldsymbol{\eta}) := \sum_{j \in \mathbb{Z}} \Phi^j \eta_j$$

the *value of the w-NAF $\boldsymbol{\eta}$*.

The following notations and conventions are used. A block of digits zero is denoted by $\mathbf{0}$. For a digit η and $k \in \mathbb{N}_0$ we will use

$$\eta^k := \underbrace{\eta \ldots \eta}_{k},$$

with the convention $\eta^0 := \varepsilon$, where ε denotes the empty word. A w-NAF $\boldsymbol{\eta} = (\eta_j)_{j \in \mathbb{Z}}$ will be written as $\boldsymbol{\eta}_I.\boldsymbol{\eta}_F$, where $\boldsymbol{\eta}_I$ contains the η_j with $j \geq 0$ and $\boldsymbol{\eta}_F$ contains the η_j with $j < 0$. $\boldsymbol{\eta}_I$ is called *integer part*, $\boldsymbol{\eta}_F$ *fractional part*, and the dot is called *Φ-point*. Left-leading zeros in $\boldsymbol{\eta}_I$ can be skipped, except η_0, and right-leading zeros in $\boldsymbol{\eta}_F$ can be skipped as well. If $\boldsymbol{\eta}_F$ is a sequence containing only zeros, the Φ-point and this sequence is not drawn.

Further, for a w-NAF $\boldsymbol{\eta}$ (a bold, usually small Greek letter) we will always use η_j (the same letter, but indexed and not bold) for the elements of the sequence.

The set $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$ can be equipped with a metric. It is defined in the following way. Let $\rho > 1$. For $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ and $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ define

$$\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \boldsymbol{\xi}) := \begin{cases} \rho^{\max\{j \in \mathbb{Z} \,:\, \eta_j \neq \xi_j\}} & \text{if } \boldsymbol{\eta} \neq \boldsymbol{\xi}, \\ 0 & \text{if } \boldsymbol{\eta} = \boldsymbol{\xi}. \end{cases}$$

So the largest index, where the two w-NAFs differ, decides their distance. See for example Edgar [9] for details on such metrics.

We get a compactness result on the metric space $\mathbf{NAF}_w^{\ell.\infty} \subseteq \mathbf{NAF}_w^{\mathsf{fin}.\infty}$, $\ell \in \mathbb{N}_0$, see the proposition below. The metric space $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$ is not compact, because if we fix a non-zero digit η, then the sequence $\left(\eta 0^j\right)_{j \in \mathbb{N}_0}$ has no convergent subsequence, but all $\eta 0^j$ are in the set $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$.

Proposition 2.3. *For every $\ell \geq 0$ the metric space $\left(\mathbf{NAF}_w^{\ell.\infty}, \mathrm{d}_{\mathsf{NAF}}\right)$ is compact.*

This is a consequence of Tychonoff's Theorem, see [12] for details.

3. The Set-Up and Notations

In this section we describe the set-up, which we use throughout this article.

(1) Let Λ be a lattice in $\mathbb{R}^n$ with full rank, i.e., $\Lambda = w_1 \mathbb{Z} \oplus \cdots \oplus w_n \mathbb{Z}$ for linearly independent $w_1, \ldots, w_n \in \mathbb{R}^n$.

(2) Let $n \in \mathbb{N}$ and Φ be an endomorphism of $\mathbb{R}^n$ with $\Phi(\Lambda) \subseteq \Lambda$. We assume that each eigenvalue of Φ has the same absolute value ρ, where ρ is a fixed real constant with $\rho > 1$. Further we assume that $\rho^n \in \mathbb{N}$. Additionally, we take this ρ as parameter in the definition of the metric $\mathrm{d}_{\mathsf{NAF}}$.

(3) Suppose that the set $T \subseteq \mathbb{R}^n$ tiles the space $\mathbb{R}^n$ by the lattice Λ, i.e., the following two properties hold:
  (a) $\bigcup_{z \in \Lambda}(z + T) = \mathbb{R}^n$,
  (b) $T \cap (z + T) \subseteq \partial T$ holds for all $z \in \Lambda$ with $z \neq 0$.
  Further, we assume that T is closed and that $\lambda(\partial T) = 0$, where λ denotes the n-dimensional Lebesgue measure. We set $d_\Lambda := \lambda(T)$.

(4) Let $\|\cdot\|$ be a vector norm on $\mathbb{R}^n$ such that for the corresponding induced operator norm, also denoted by $\|\cdot\|$, the equalities $\|\Phi\| = \rho$ and $\left\|\Phi^{-1}\right\| = \rho^{-1}$ hold.

  For a $z \in \Lambda$ and non-negative $r \in \mathbb{R}$ the *open ball with centre z and radius r* is denoted by

$$\mathcal{B}(z, r) := \{y \in \Lambda \,:\, \|z - y\| < r\}$$

  and the *closed ball with centre z and radius r* by

$$\overline{\mathcal{B}}(z, r) := \{y \in \Lambda \,:\, \|z - y\| \leq r\}.$$

(5) Let r and R be positive reals with

$$\overline{\mathcal{B}}(0, r) \subseteq T \subseteq \overline{\mathcal{B}}(0, R). \tag{3.1}$$

(6) Let w be a positive integer such that

$$\frac{R}{r} < \rho^w - 1. \tag{3.2}$$

(7) Let $\mathcal{D}$ be a reduced residue digit set modulo Φ^w, cf. Definition 2.1, corresponding to the tiling T, i.e. the digit set $\mathcal{D}$ fulfils $\mathcal{D} \subseteq \Phi^w T$.

  Further, suppose that the cardinality of the digit set $\mathcal{D}$ is

$$\rho^{n(w-1)} \left(\rho^n - 1\right) + 1.$$

We use the following notation concerning our tiling: for a lattice element $z \in \Lambda$ we set $T_z := z + T$. Therefore $\bigcup_{z \in \Lambda} T_z = \mathbb{R}^n$ and $T_y \cap T_z \subseteq \partial T_z$ for all distinct $y, z \in \Lambda$.

Next we define a fractional part function in $\mathbb{R}^n$ with respect to the lattice Λ, which should be a generalisation of the usual fractional part of elements in $\mathbb{R}$ with respect to the rational integers $\mathbb{Z}$. Our tiling T induces such a fractional part.

Definition 3.1 (Fractional Part). Let $\widetilde{T}$ be a tiling arising from T in the following way: Restrict the set $\widetilde{T} \subseteq T$ such that it fulfils $\biguplus_{z \in \Lambda} (z + \widetilde{T}) = \mathbb{R}^n$.

For $z \in \mathbb{R}^n$ with $z = u + v$, where $u \in \Lambda$ and $v \in \widetilde{T}$ define the *fractional part corresponding to the lattice* Λ by $\{z\}_\Lambda := v$.

Note that this fractional part depends on the tiling T (or more precisely, on the tiling $\widetilde{T}$). We omit this dependency, since we assume that our tiling is fixed.

4. Some Basic Properties and some Remarks

The previous section contained our set-up. Some basic implications of that set-up are now given in this section. Further we give remarks on the tilings and on the digit sets used, and there are also comments on the existence of w-NAF-expansions in the lattice.

We start with two remarks on our mapping Φ.

Remark 4.1. Since all eigenvalues of Φ have an absolute value larger than 1, the function Φ is injective.

Remark 4.2. We have assumed $\|\Phi\| = \rho$ and $\|\Phi^{-1}\| = \rho^{-1}$. Therefore, for all $J \in \mathbb{Z}$ the equality $\|\Phi^J\| = \rho^J$ follows.

Remark 4.3. The endomorphism Φ is diagonalisable. This follows from the assumptions that all eigenvalues have the same absolute value ρ and the existence of a norm with $\|\Phi\| = \rho$.

One special tiling comes from the Voronoi diagram of the lattice. This is stated in the remark below.

Remark 4.4. Let
$$V := \{z \in \mathbb{R}^n \,:\, \forall y \in \Lambda : \|z\| \leq \|z - y\|\}.$$
We call V the *Voronoi cell for* 0 corresponding to the lattice Λ. Let $u \in \Lambda$. We define the *Voronoi cell for* u as $V_u := u + V$.

Now choosing $T = V$ results in a tiling of the $\mathbb{R}^n$ by the lattice Λ.

In our set-up the digit set corresponds to the tiling. In Remark 4.5 this is explained in more details. The Voronoi tiling mentioned above gives rise to a special digit set, namely the minimal norm digit set. There, for each digit a representative of minimal norm is chosen.

Remark 4.5. The condition $\frac{R}{r} < \rho^w - 1$ in the our set-up implies the existence of w-NAFs: each element of Λ has a unique w-NAF-expansion with the digit set $\mathcal{D}$. See Heuberger and Krenn [14] for details. There numeral systems in lattices with w-NAF-condition and digit sets coming from tilings are explained in detail. Further it is shown that each tiling and positive integer w give rise to a digit set $\mathcal{D}$.

Because $\mathcal{D} \subseteq \Phi^w T$, we have
$$\rho^w r \leq \|d\| \leq \rho^w R$$
for each non-zero digit $d \in \mathcal{D}$.

Further, we get the following continuity result.

Proposition 4.6. *The value function* value *is Lipschitz continuous on* $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$.

This result is a consequence of the boundedness of the digit set, see [12] for a formal proof.

We need the full block length distribution theorem from Heuberger and Krenn [12]. This was proved for numeral systems with algebraic integer τ as base. But the result does not depend on τ directly, only on the size of the digit set, which is dependent on the norm of τ. In our case this norm equals ρ^n. That replacement is already done in the theorem written down below.

Theorem 4.7 (Full Block Length Distribution Theorem). *Denote the number of w-NAFs of length $m \in \mathbb{N}_0$ by C_m. We get*

$$C_m = \frac{1}{(\rho^n - 1)w + 1} \rho^{n(m+w)} + \mathcal{O}((\mu\rho^n)^m),$$

where $\mu = (1 + \frac{1}{\rho^n w^3})^{-1} < 1$.

Further let $0 \neq \eta \in \mathcal{D}$ be a fixed digit and define the random variable $X_{m,\eta}$ to be the number of occurrences of the digit η in a random w-NAF of length m, where every w-NAF of length m is assumed to be equally likely. Then we get

$$\mathbb{E}(X_{m,\eta}) = Em + \mathcal{O}(1)$$

for the expectation, where

$$E = \frac{1}{\rho^{n(w-1)}((\rho^n - 1)w + 1)}.$$

The theorem in [12] gives more details, which we do not need for the results in this article: We have

$$\mathbb{E}(X_{m,\eta}) = Em + E_0 + \mathcal{O}(m\mu^m)$$

with an explicit constant term E_0. Further the variance

$$\mathbb{V}(X_{n,w,\eta}) = Vm + V_0 + \mathcal{O}(m^2\mu^m)$$

with explicit constants V and V_0 is calculated, and a central limit theorem is proved.

5. BOUNDS FOR THE VALUE OF NON-ADJACENT FORMS

In this section we have a closer look at the value of a w-NAF. We want to find upper bounds, as well as, a lower bound for it. In the proofs of all those bounds we use bounds for the norm $\|\cdot\|$. More precisely, geometric parameters of the tiling T, i.e., the already defined reals r and R, are used.

The following proposition deals with three upper bounds, one for the norm of the value of a w-NAF-expansion and two give us bounds in conjunction with the tiling.

Proposition 5.1 (Upper Bounds). *Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$, and denote the position of the most significant digit of $\boldsymbol{\eta}$ by J. Let*

$$B_U = \frac{\rho^w R}{1 - \rho^{-w}}.$$

Then the following statements are true:

(a) We get

$$\|\mathsf{value}(\boldsymbol{\eta})\| \leq \rho^J B_U$$

(b) We have

$$\mathsf{value}(\boldsymbol{\eta}) \in \bigcup_{z \in \Phi^{w+J} T} \overline{\mathcal{B}}(z, \rho^{-w+J} B_U).$$

(c) We get
$$\mathsf{value}(\boldsymbol{\eta}) \in \Phi^{2w+J}T.$$

(d) For each $\ell \in \mathbb{N}_0$ we have
$$\mathsf{value}(0.\eta_{-1}\dots\eta_{-\ell}) + \Phi^{-\ell}T \subseteq \Phi^{2w-1}T.$$

Note that $\rho^J = \mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \mathbf{0})$, so we can rewrite the statements of the proposition above in terms of that metric, see also Corollary 5.3.

Proof. (a) In the calculations below, we use the Iversonian notation $[expr] = 1$ if *expr* is true and $[expr] = 0$ otherwise, cf. Graham, Knuth and Patashnik [11].

The result follows trivially for $\boldsymbol{\eta} = \mathbf{0}$. First assume that the most significant digit of $\boldsymbol{\eta}$ is at position 0. Since $\|\eta_{-j}\| \leq \rho^w R$, see Remark 4.5 on page 5, $\rho > 1$ and $\boldsymbol{\eta}$ is fulfilling the w-NAF-condition we obtain

$$\|\mathsf{value}(\boldsymbol{\eta})\| = \left\|\sum_{j=0}^{\infty} \Phi^{-j}\eta_{-j}\right\| \leq \sum_{j=0}^{\infty} \left\|\Phi^{-1}\right\|^j \|\eta_{-j}\| = \sum_{j=0}^{\infty} \rho^{-j} \|\eta_{-j}\|$$

$$\leq \rho^w R \sum_{j=0}^{\infty} \rho^{-j} [\eta_{-j} \neq 0] \leq \rho^w R \sum_{j=0}^{\infty} \rho^{-j} [-j \equiv 0 \ (\mathrm{mod}\ w)]$$

$$= \rho^w R \sum_{k=0}^{\infty} \rho^{-wk} = \frac{\rho^w R}{1 - \rho^{-w}} = B_U.$$

In the general case we have the most significant digit of $\boldsymbol{\eta}$ at a position J. Then $\mathsf{value}(\boldsymbol{\eta}) = \Phi^J \mathsf{value}(\boldsymbol{\eta}')$ for a w-NAF $\boldsymbol{\eta}'$ with most significant digit at position 0. Therefore

$$\|\mathsf{value}(\boldsymbol{\eta})\| = \left\|\Phi^J \mathsf{value}(\boldsymbol{\eta}')\right\| \leq \|\Phi\|^J \|\mathsf{value}(\boldsymbol{\eta}')\| \leq \rho^J B_U,$$

which was to prove.

(b) There is nothing to show if the w-NAF $\boldsymbol{\eta}$ is zero. First suppose that the most significant digit is at position w. Then, using (a), we have
$$\|\mathsf{value}(\boldsymbol{\eta}) - \Phi^w \eta_w\| \leq B_U,$$

therefore
$$\mathsf{value}(\boldsymbol{\eta}) \in \overline{\mathcal{B}}(\Phi^w \eta_w, B_U).$$

Since $\eta_w \in \Phi^w T$, the statement follows for the special case. The general case is again obtained by shifting.

(c) Using the upper bound found in (a) and the assumption (3.2) yields
$$\|\mathsf{value}(\boldsymbol{\eta})\| \leq \rho^J B_U = \rho^J \frac{\rho^w R}{1 - \rho^{-w}} \leq r\rho^{2w+J}.$$

Since $\overline{\mathcal{B}}(0, r\rho^{2w+J}) \subseteq \Phi^{2w+J}T$, the statement follows.

(d) Analogously to the proof of (a), except that we use ℓ for the upper bound of the sum, we obtain for $v \in T$

$$\left\|\mathsf{value}(0.\eta_{-1}\dots\eta_{-\ell}) + \Phi^{-\ell}v\right\| \leq \|\mathsf{value}(0.\eta_{-1}\dots\eta_{-\ell})\| + \rho^{-\ell}R$$

$$\leq \rho^{-1}\frac{\rho^w R}{1 - \rho^{-w}}\left(1 - \rho^{-w\lfloor\frac{\ell-1+w}{w}\rfloor}\right) + \rho^{-\ell}R$$

$$\leq \frac{\rho^{w-1}R}{1 - \rho^{-w}}\left(1 - \rho^{-\ell+1-w} + \rho^{-\ell+1-w}\left(1 - \rho^{-w}\right)\right)$$

$$= \frac{\rho^{w-1}R}{1 - \rho^{-w}}\left(1 - \rho^{-\ell+1-2w}\right).$$

Since $1 - \rho^{-\ell+1-2w} < 1$ we get

$$\left\|\mathsf{value}(0.\eta_{-1}\dots\eta_{-\ell}) + \Phi^{-\ell}T\right\| \le \rho^{-1}\frac{\rho^w R}{1 - \rho^{-w}} = \rho^{-1}B_U$$

for all $\ell \in \mathbb{N}_0$. By the same argumentation as in the proof of (c), the statement follows. $\square$

Next we want to find a lower bound for the value of a w-NAF. Clearly the w-NAF $\mathbf{0}$ has value 0, so we are interested in cases where we have a non-zero digit somewhere.

Proposition 5.2 (Lower Bound). *Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin.}\infty}$ be non-zero, and denote the position of the most significant digit of $\boldsymbol{\eta}$ by J. Then we have*

$$\|\mathsf{value}(\boldsymbol{\eta})\| \ge \rho^J B_L,$$

where

$$B_L = r - \rho^{-2w}B_U = r - \frac{R}{\rho^w - 1}.$$

Note that $B_L > 0$ is equivalent to $\frac{R}{r} < \rho^w - 1$, i.e. the assumption (3.2). Moreover, we have

$$\frac{R}{r - B_L} = \rho^w - 1.$$

Proof of Proposition 5.2. First suppose the most significant digit of the w-NAF $\boldsymbol{\eta}$ is at position 0 and the second non-zero digit (read from left to right) at position J. Then

$$\mathsf{value}(\boldsymbol{\eta}) - \eta_0 = \sum_{k=w}^{\infty} \Phi^{-k}\eta_{-k} \in \bigcup_{z \in T}\overline{\mathcal{B}}\left(z, \rho^{-w+J}B_U\right) \subseteq \bigcup_{z \in T}\overline{\mathcal{B}}\left(z, \rho^{-2w}B_U\right)$$

according to (b) of Proposition 5.1 on page 6. Therefore

$$\mathsf{value}(\boldsymbol{\eta}) \in \bigcup_{z \in T_{\eta_0}}\overline{\mathcal{B}}\left(z, \rho^{-2w}B_U\right).$$

This means that $\mathsf{value}(\boldsymbol{\eta})$ is in T_{η_0} or in a $\rho^{-2w}B_U$-strip around this cell. The two tiling cells T_{η_0} for η_0 and $T_0 = T$ for 0 are disjoint, except for parts of the boundary, if they are adjacent. Since a ball with radius r is contained in each tiling cell, we deduce that

$$\|\mathsf{value}(\boldsymbol{\eta})\| \ge r - \rho^{-2w}B_U = r - \frac{R}{\rho^w - 1} = B_L,$$

which was to show. The case of a general J is again, as in the proof of Proposition 5.1 obtained by shifting. $\square$

Combining the previous two propositions leads to the following corollary, which gives an upper and a lower bound for the norm of the value of a w-NAF by looking at the largest non-zero index.

Corollary 5.3 (Bounds for the Value). *Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin.}\infty}$, then we get*

$$\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \mathbf{0})\, B_L \le \|\mathsf{value}(\boldsymbol{\eta})\| \le \mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \mathbf{0})\, B_U.$$

Proof. Follows directly from Proposition 5.1 on page 6 and Proposition 5.2, since the term ρ^J is equal to $\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \mathbf{0})$. $\square$

Last in this section, we want to find out if there are special w-NAFs for which we know for sure that all their expansions start with a certain finite w-NAF. This is formulated in the following lemma.

Lemma 5.4. *There is a $k_0 \in \mathbb{N}_0$ such that for all $k \geq k_0$ the following holds: If $\boldsymbol{\eta} \in \mathbf{NAF}_w^{0.\infty}$ starts with the word 0^k, i.e., $\eta_{-1} = 0, \ldots, \eta_{-k} = 0$, then we get for all $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathrm{fin}.\infty}$ that $\mathsf{value}(\boldsymbol{\xi}) = \mathsf{value}(\boldsymbol{\eta})$ implies $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$.*

Proof. Let $\boldsymbol{\xi} = \boldsymbol{\xi}_I.\boldsymbol{\xi}_F$. Then $\|\mathsf{value}(\boldsymbol{\xi}_I.\boldsymbol{\xi}_F)\| < B_L$ implies $\boldsymbol{\xi}_I = \mathbf{0}$, cf. Corollary 5.3. Further, for our $\boldsymbol{\eta}$ we obtain $z = \|\mathsf{value}(\boldsymbol{\eta})\| \leq \rho^{-k} B_U$. So it is sufficient to show that

$$\rho^{-k} B_U < B_L,$$

which is equivalent to

$$k > \log_\rho \frac{B_U}{B_L}.$$

We obtain

$$k > 2w - \log_\rho \left(\frac{r}{R} (\rho^w - 1) - 1 \right),$$

where we just inserted the formulas for B_U and B_L. Choosing an appropriate k_0 is now easily possible. $\qquad\square$

Note that the we can find a constant k_1 independent from w such that for all $k \geq 2w + k_1$ the assertion of Lemma 5.4 holds. This can be seen in the proof, since $\frac{r}{R}(\rho^w - 1) - 1$ is monotonically increasing in w.

6. Right-infinite Expansions

We have the existence of a (finite integer) w-NAF-expansion for each element of the lattice $\Lambda \subseteq \mathbb{R}^n$, cf. Remark 4.5. But that existence condition is also sufficient to get w-NAF-expansions for all elements in $\mathbb{R}^n$. Those expansions possibly have an infinite right-length. The aim of this section is to show that result. The proofs themselves are a minor generalisation of the ones given in [12] for the quadratic case.

We will use the following abbreviation in this section. We define

$$[\Phi^{-1}]\Lambda := \bigcup_{j \in \mathbb{N}_0} \Phi^{-j}\Lambda.$$

Note that $\Lambda \subseteq \Phi^{-1}\Lambda$.

To prove the existence theorem of this section, we need the following three lemmata.

Lemma 6.1. *The function $\mathsf{value}|_{\mathbf{NAF}_w^{\mathrm{fin.fin}}}$ is injective.*

Proof. Let $\boldsymbol{\eta}$ and $\boldsymbol{\xi}$ be elements of $\mathbf{NAF}_w^{\mathrm{fin.fin}}$ with $\mathsf{value}(\boldsymbol{\eta}) = \mathsf{value}(\boldsymbol{\xi})$. This implies that $\Phi^J \mathsf{value}(\boldsymbol{\eta}) = \Phi^J \mathsf{value}(\boldsymbol{\xi}) \in \Lambda$ for some $J \in \mathbb{Z}$. By uniqueness of the integer w-NAFs we conclude that $\boldsymbol{\eta} = \boldsymbol{\xi}$. $\qquad\square$

Lemma 6.2. *We have $\mathsf{value}\left(\mathbf{NAF}_w^{\mathrm{fin.fin}}\right) = [\Phi^{-1}]\Lambda$.*

Proof. Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathrm{fin.fin}}$. There are only finitely many $\eta_j \neq 0$, so there is a $J \in \mathbb{N}_0$ such that $\mathsf{value}(\boldsymbol{\eta}) \in \Phi^{-J}\Lambda$. Conversely, if $z \in \Phi^{-J}\Lambda$, then there is an integer w-NAF of $\Phi^J z$, and therefore, there is a $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathrm{fin.fin}}$ with $\mathsf{value}(\boldsymbol{\xi}) = z$. $\qquad\square$

Lemma 6.3. *$[\Phi^{-1}]\Lambda$ is dense in $\mathbb{R}^n$.*

Proof. Let $\Lambda = w_1 \mathbb{Z} \oplus \cdots \oplus w_n \mathbb{Z}$ for linearly independent $w_1, \ldots, w_n \in \mathbb{R}^n$. Let $z \in \mathbb{R}^n$ and $K \in \mathbb{N}_0$. Then $\Phi^K z = z_1 w_1 + \cdots + z_n w_n$ for some reals $z_1, \ldots, z_n$. We have

$$\left\| z - \left(\lfloor z_1 \rfloor \Phi^{-K} w_1 + \cdots + \lfloor z_n \rfloor \Phi^{-K} w_n \right) \right\| < \rho^{-K} \left(\|w_1\| + \cdots + \|w_n\| \right),$$

which proves the lemma. $\qquad\square$

Now we can prove the following theorem.

Theorem 6.4 (Existence Theorem concerning $\mathbb{R}^n$). *Let $z \in \mathbb{R}^n$. Then there is an $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ such that $z = \mathsf{value}(\boldsymbol{\eta})$, i.e., each element in $\mathbb{R}^n$ has a w-NAF-expansion.*

Proof. By Lemma 6.3 on the preceding page, there is a sequence $z_n \in [\Phi^{-1}]\Lambda$ converging to z. By Lemma 6.2 on the previous page, there is a sequence $\boldsymbol{\eta}_n \in \mathbf{NAF}_w^{\mathsf{fin}.\mathsf{fin}}$ with $\mathsf{value}(\boldsymbol{\eta}_n) = z_n$ for all n. By Corollary 5.3 on page 8 the sequence $\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}_n, 0)$ is bounded from above, so there is an ℓ such that $\boldsymbol{\eta}_n \in \mathbf{NAF}_w^{\ell.\mathsf{fin}} \subseteq \mathbf{NAF}_w^{\ell.\infty}$. By Proposition 2.3 on page 4, we conclude that there is a convergent subsequence $\boldsymbol{\eta}_n'$ of $\boldsymbol{\eta}_n$. Set $\boldsymbol{\eta} := \lim_{n\to\infty} \boldsymbol{\eta}_n'$. By continuity of value, see Proposition 4.6 on page 6, we conclude that $\mathsf{value}(\boldsymbol{\eta}) = z$. $\qquad\square$

7. The Fundamental Domain

We now derive properties of the *Fundamental Domain*, i.e., the subset of $\mathbb{R}^n$ representable by w-NAFs which vanish left of the Φ-point. The boundary of the fundamental domain is shown to correspond to elements which admit more than one w-NAFs differing left of the Φ-point. Finally, an upper bound for the Hausdorff dimension of the boundary is derived.

All the results in this section are generalisations of the propositions and remarks found in [12]. For some of those results given here, the proof is a the same as in the quadratic case or a straight forward generalisation of it. In those cases the proofs will be skipped.

We start with the formal definition of the fundamental domain.

Definition 7.1 (Fundamental Domain). The set

$$\mathcal{F} := \mathsf{value}\big(\mathbf{NAF}_w^{0.\infty}\big) = \big\{\mathsf{value}(\boldsymbol{\xi}) \,:\, \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}\big\}.$$

is called *fundamental domain*.

The pictures in Figure 9.1 on page 16 show some fundamental domains for lattices coming from imaginary-quadratic algebraic integers τ. We continue with some properties of fundamental domains. We have the following compactness result.

Proposition 7.2. *The fundamental domain $\mathcal{F}$ is compact.*

Proof. The proof is a straight forward generalisation of the proof of the quadratic case in [12]. $\qquad\square$

We can also compute the Lebesgue measure of the fundamental domain. This result can be found in Remark 9.3 on page 17. To calculate $\lambda(\mathcal{F})$, we will need the results of Sections 8 and 9.

The space $\mathbb{R}^n$ has a tiling property with respect to the fundamental domain. This fact is stated in the following proposition.

Proposition 7.3 (Tiling Property). *The space $\mathbb{R}^n$ can be tiled with scaled versions of the fundamental domain $\mathcal{F}$. Only finitely many different size are needed. More precisely: Let $K \in \mathbb{Z}$, then*

$$\mathbb{R}^n = \bigcup_{\substack{k \in \{K, K+1, \ldots, K+w-1\} \\ \boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.0} \\ k \neq K+w-1 \; implies \; \boldsymbol{\xi}_0 \neq 0}} \big(\Phi^k\, \mathsf{value}(\boldsymbol{\xi}) + \Phi^{k-w+1}\mathcal{F}\big),$$

and the intersection of two different $\Phi^k\, \mathsf{value}(\boldsymbol{\xi}) + \Phi^{k-w+1}\mathcal{F}$ in this union is a subset of the intersection of their boundaries.

Proof. The proof is a straight forward generalisation of the proof of the quadratic case in [12]. □

Note that the intersection of the two different sets of the tiling in the previous corollary has Lebesgue measure 0. This will be a consequence of Proposition 7.6.

Remark 7.4 (Iterated Function System). Define $f_0(z) = \Phi^{-1}z$ and for a non-zero digit $\vartheta \in \mathcal{D}^\bullet$ define $f_\vartheta(z) = \Phi^{-1}\vartheta + \Phi^{-w}z$. Then the *(affine) iterated function system* $(f_\vartheta)_{\vartheta \in \mathcal{D}}$, cf. Edgar [9] or Barnsley [2], has the fundamental domain $\mathcal{F}$ as an invariant set, i.e.,

$$\mathcal{F} = \bigcup_{\vartheta \in \mathcal{D}} f_\vartheta(\mathcal{F}) = \Phi^{-1}\mathcal{F} \cup \bigcup_{\vartheta \in \mathcal{D}^\bullet} \left(\Phi^{-1}\vartheta + \Phi^{-w}\mathcal{F}\right).$$

That formula also reflects the fact that we have two possibilities building the elements $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$ from left to right: We can either append 0, what corresponds to an application of Φ^{-1}, or we can append a non-zero digit $\vartheta \in \mathcal{D}^\bullet$ and then add $w-1$ zeros.

Furthermore, the iterated function system $(f_\vartheta)_{\vartheta \in \mathcal{D}}$ fulfils *Moran's open set condition*[1], cf. Edgar [9] or Barnsley [2]. The *Moran open set* used is $\operatorname{int} \mathcal{F}$. This set satisfies

$$f_\vartheta(\operatorname{int} \mathcal{F}) \cap f_{\vartheta'}(\operatorname{int} \mathcal{F}) = \emptyset$$

for $\vartheta \neq \vartheta' \in \mathcal{D}$ and

$$\operatorname{int} \mathcal{F} \supseteq f_\vartheta(\operatorname{int} \mathcal{F})$$

for all $\vartheta \in \mathcal{D}$. We remark that the first condition follows directly from the tiling property in Corollary 7.3 on the facing page with $K = -1$. The second condition follows from the fact that f_ϑ is an open mapping.

Next we want to have a look at the Hausdorff dimension of the boundary of $\mathcal{F}$. We will need the following characterisation of the boundary.

Proposition 7.5 (Characterisation of the Boundary)**.** *Let $z \in \mathcal{F}$. Then $z \in \partial\mathcal{F}$ if and only if there exists a w-NAF $\boldsymbol{\xi}_I.\boldsymbol{\xi}_F \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ with $\boldsymbol{\xi}_I \neq \mathbf{0}$ such that $z = \mathsf{value}(\boldsymbol{\xi}_I.\boldsymbol{\xi}_F)$.*

Proof. The proof is a straight forward generalisation of the proof of the quadratic case in [12]. □

The following proposition deals with the Hausdorff dimension of the boundary of $\mathcal{F}$.

Proposition 7.6. *For the Hausdorff dimension of the boundary of the fundamental domain we get $\dim_H \partial\mathcal{F} < n$.*

The idea of this proof is similar to a proof in Heuberger and Prodinger [15], and it is a generalisation of the one given in [12].

Proof. Set $k := k_0 + w - 1$ with k_0 from Lemma 5.4 on page 9. For $j \in \mathbb{N}$ define

$$U_j := \left\{\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.j} : \xi_{-\ell}\xi_{-(\ell+1)}\cdots\xi_{-(\ell+k-1)} \neq 0^k \text{ for all } \ell \in \{1, \ldots, j-k+1\}\right\}.$$

The elements of U_j, or more precisely the digits from index -1 to $-j$, can be described by the regular expression

$$\left(\varepsilon + \sum_{d \in \mathcal{D}^\bullet} \sum_{\ell=0}^{w-2} 0^\ell d\right) \left(\sum_{d \in \mathcal{D}^\bullet} \sum_{\ell=w-1}^{k-1} 0^\ell d\right)^* \left(\sum_{\ell=0}^{k-1} 0^\ell\right).$$

---

[1]"Moran's open set condition" is sometimes just called "open set condition"
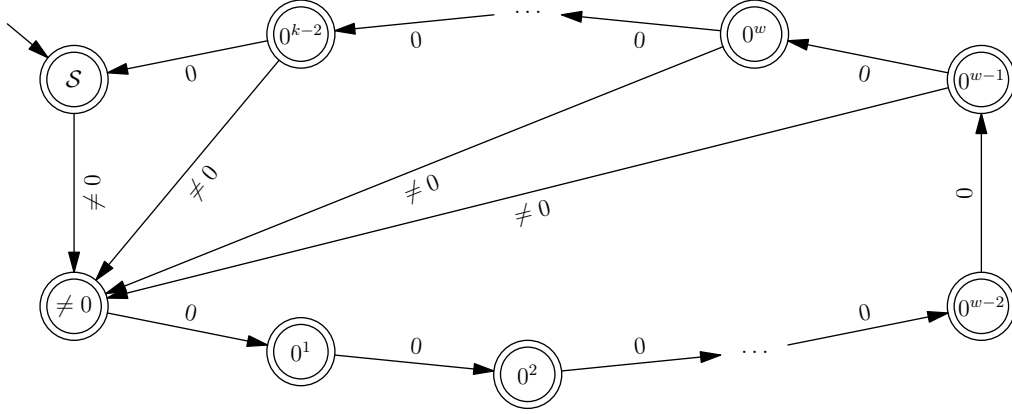
FIGURE 7.1. Automaton $\mathcal{A}$ recognising $\bigcup_{j \in \mathbb{N}} \widetilde{U}_j$ from right to left, see proof of Proposition 7.6. The state $\mathcal{S}$ is the starting state, all states are valid end states. An edge marked with $\neq 0$ means one edge for each non-zero digit in the digit set $\mathcal{D}$. The state $\neq 0$ means that there was an non-zero digit read, a state 0^ℓ means that ℓ zeros have been read.

This can be translated to the generating function

$$G(Z) = \sum_{j \in \mathbb{N}} \#U_j Z^j = \left(1 + \#\mathcal{D}^\bullet \sum_{\ell=0}^{w-2} Z^{\ell+1} \right) \frac{1}{1 - \#\mathcal{D}^\bullet \sum_{\ell=w-1}^{k-1} Z^{\ell+1}} \left(\sum_{\ell=0}^{k-1} Z^\ell \right)$$

used for counting the number of elements in U_j. Rewriting yields

$$G(Z) = \frac{1 - Z^k}{1 - Z} \frac{1 + (\#\mathcal{D}^\bullet - 1)Z - \#\mathcal{D}^\bullet Z^w}{1 - Z - \#\mathcal{D}^\bullet Z^w + \#\mathcal{D}^\bullet Z^{k+1}},$$

and we set

$$q(Z) := 1 - Z - \#\mathcal{D}^\bullet Z^w + \#\mathcal{D}^\bullet Z^{k+1}.$$

Now we define

$$\widetilde{U}_j := \{ \boldsymbol{\xi} \in U_j \, : \, \xi_{-j} \neq 0 \}$$

and consider $\widetilde{U} := \bigcup_{j \in \mathbb{N}} \widetilde{U}_j$. Suppose $w \geq 2$. The w-NAFs in that set, or more precisely the finite strings from index -1 to the smallest index of a non-zero digit, will be recognised by the automaton $\mathcal{A}$ which is shown in Figure 7.1 and reads its input from right to left. It is easy to see that the underlying directed graph $G_{\mathcal{A}}$ of the automaton $\mathcal{A}$ is strongly connected, therefore its adjacency matrix $M_{\mathcal{A}}$ is irreducible. Since there are cycles of length w and $w + 1$ in the graph and $\gcd(w, w+1) = 1$, the adjacency matrix is primitive. Thus, using the Perron-Frobenius theorem we obtain

$$\#\widetilde{U}_j = \#(\text{walks in } G_{\mathcal{A}} \text{ of length } j \text{ from starting state } \mathcal{S} \text{ to some other state})$$

$$= \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix} M_{\mathcal{A}}^j \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \widetilde{c} (\sigma \rho^n)^j \left(1 + \mathcal{O}(s^j) \right)$$

for a $\widetilde{c} > 0$, a $\sigma > 0$, and an s with $0 \leq s < 1$. Since the number of w-NAFs of length j is $\mathcal{O}(\rho^{nj})$, see Theorem 4.7 on page 6, we get $\sigma \leq 1$.

We clearly have

$$U_j = \biguplus_{\ell=j-k+1}^{j} \widetilde{U}_\ell,$$

so we get

$$\#U_j = \left[Z^j\right] G(Z) = c\,(\sigma\rho^n)^j \left(1 + \mathcal{O}(s^j)\right)$$

for some constant $c > 0$.

To rule out $\sigma = 1$, we insert the "zero" ρ^{-n} in $q(Z)$. We obtain

$$\begin{aligned}
q(\rho^{-n}) &= 1 - \rho^{-n} - \#\mathcal{D}^\bullet \rho^{-nw} + \#\mathcal{D}^\bullet \rho^{-n(k+1)} \\
&= 1 - \rho^{-n} - \rho^{n(w-1)}\left(\rho^n - 1\right)\rho^{-nw} + \rho^{n(w-1)}\left(\rho^n - 1\right)\rho^{-n(k+1)} \\
&= \left(\rho^n - 1\right)\rho^{n(w-k-2)} > 0,
\end{aligned}$$

where we used the cardinality of $\mathcal{D}^\bullet$ from our set-up in Section 3 and $\rho > 1$. Therefore we get $\sigma < 1$. It is easy to check, that the result for $\#U_j$ holds in the case $w = 1$, too.

Define

$$U := \left\{\mathsf{value}(\boldsymbol{\xi}) \,:\, \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty} \text{ with } \xi_{-\ell}\xi_{-(\ell+1)}\cdots\xi_{-(\ell+k-1)} \neq 0^k \text{ for all } \ell \geq 1\right\}.$$

We want to cover U with hypercubes. Let $C \subseteq \mathbb{R}^n$ be the closed paraxial hypercube with centre 0 and width 2. Using Proposition 5.1 on page 6 yields

$$U \subseteq \bigcup_{z \in \mathsf{value}(U_j)} \left(z + B_U \rho^{-j} C\right)$$

for all $j \in \mathbb{N}$, i.e., U can be covered with $\#U_j$ boxes of size $2B_U\rho^{-j}$. Thus we get for the upper box dimension, cf. Edgar [9],

$$\overline{\dim}_B U \leq \lim_{j\to\infty} \frac{\log \#U_j}{-\log(2B_U\rho^{-j})}.$$

Inserting the cardinality $\#U_j$ from above, using the logarithm to base ρ and $0 \leq s < 1$ yields

$$\overline{\dim}_B U \leq \lim_{j\to\infty} \frac{\log_\rho c + j\log_\rho(\sigma\rho^n) + \log_\rho(1 + \mathcal{O}(s^j))}{j + \mathcal{O}(1)} = n + \log_\rho \sigma.$$

Since $\sigma < 1$, we get $\overline{\dim}_B U < 2$.

Now we will show that $\partial\mathcal{F} \subseteq U$. Clearly $U \subseteq \mathcal{F}$, so the previous inclusion is equivalent to $\mathcal{F} \setminus U \subseteq \mathsf{int}(\mathcal{F})$. So let $z \in \mathcal{F} \setminus U$. Then there is a $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$ such that $z = \mathsf{value}(\boldsymbol{\xi})$ and $\boldsymbol{\xi}$ has a block of at least k zeros somewhere on the right hand side of the Φ-point. Let ℓ denote the starting index of this block, i.e.,

$$\boldsymbol{\xi} = 0.\underbrace{\xi_{-1}\ldots\xi_{-(\ell-1)}}_{=:\boldsymbol{\xi}_A} 0^k \xi_{-(\ell+k)}\xi_{-(\ell+k+1)}\cdots.$$

Let $\boldsymbol{\vartheta} = \boldsymbol{\vartheta}_I.\boldsymbol{\vartheta}_A\vartheta_{-\ell}\vartheta_{-(\ell+1)}\ldots \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ with $\mathsf{value}(\boldsymbol{\vartheta}) = z$. We have

$$z = \mathsf{value}(0.\boldsymbol{\xi}_A) + \Phi^{-\ell-w} z_\xi = \mathsf{value}(\boldsymbol{\vartheta}_I.\boldsymbol{\vartheta}_A) + \Phi^{-\ell-w} z_\vartheta$$

for appropriate z_ξ and z_ϑ. By Lemma 5.4 on page 9, all expansions of z_ξ are in $\mathbf{NAF}_w^{0.\infty}$. Thus all expansions of

$$\mathsf{value}(\boldsymbol{\vartheta}_I\boldsymbol{\vartheta}_A) + \Phi^{-(w-1)} z_\vartheta - \mathsf{value}(\boldsymbol{\xi}_A) = \Phi^{\ell-1} z - \mathsf{value}(\boldsymbol{\xi}_A) = \Phi^{-(w-1)} z_\xi$$

start with 0.0^{w-1}, since our choice of k is $k_0 + w - 1$. As the unique w-NAF of $\mathsf{value}(\boldsymbol{\vartheta}_I\boldsymbol{\vartheta}_A) - \mathsf{value}(\boldsymbol{\xi}_A)$ concatenated with any w-NAF of $\Phi^{-(w-1)}z_\vartheta$ gives rise to such an expansion, we conclude that $\mathsf{value}(\boldsymbol{\vartheta}_I\boldsymbol{\vartheta}_A) - \mathsf{value}(\boldsymbol{\xi}_A) = 0$ and therefore $\boldsymbol{\vartheta}_I = \mathbf{0}$ and $\boldsymbol{\vartheta}_A = \boldsymbol{\xi}_A$. So we conclude that all representations of z as a w-NAF have

to be of the form $0.\boldsymbol{\xi}_A 0^{w-1}\boldsymbol{\eta}$ for some w-NAF $\boldsymbol{\eta}$. Thus, by using Proposition 7.5 on page 11, we get $z \notin \partial \mathcal{F}$ and therefore $z \in \mathrm{int}(\mathcal{F})$.

Until now we have proved

$$\overline{\dim}_B \partial \mathcal{F} \le \overline{\dim}_B U < n.$$

Because the Hausdorff dimension of a set is at most its upper box dimension, cf. Edgar [9] again, the desired result follows. $\qquad\square$

8. Cell Rounding Operations

In this section we define operators working on subsets of the space $\mathbb{R}^n$. These will use the lattice Λ and the tiling T. They will be a very useful concept to prove Theorem 10.1 on page 17.

Definition 8.1 (Cell Rounding Operations). Let $B \subseteq \mathbb{R}^n$ and $j \in \mathbb{Z}$. We define the *cell packing of B* ("floor B")

$$\lfloor B \rfloor_T := \bigcup_{\substack{z \in \Lambda \\ T_z \subseteq B}} T_z \qquad \text{and} \qquad \lfloor B \rfloor_{T,j} := \Phi^{-j}\big(\lfloor \Phi^j B \rfloor_T\big),$$

the *cell covering of B* ("ceil B")

$$\lceil B \rceil_T := \overline{\lfloor B^C \rfloor_T^C} \qquad \text{and} \qquad \lceil B \rceil_{T,j} := \Phi^{-j}\big(\lceil \Phi^j B \rceil_T\big),$$

the *fractional cells of B*

$$\{B\}_T := B \setminus \lfloor B \rfloor_T \qquad \text{and} \qquad \{B\}_{T,j} := \Phi^{-j}\big(\{\Phi^j B\}_T\big),$$

the *cell covering of the boundary of B*

$$\partial(B)_T := \overline{\lceil B \rceil_T \setminus \lfloor B \rfloor_T} \qquad \text{and} \qquad \partial(B)_{T,j} := \Phi^{-j}\big(\partial(\Phi^j B)_T\big),$$

the *cell covering of the lattice points inside B*

$$\lfloor B \rceil_T := \bigcup_{z \in B \cap \Lambda} T_z \qquad \text{and} \qquad \lfloor B \rceil_{T,j} := \Phi^{-j}\big(\lfloor \Phi^j B \rceil_T\big),$$

and the *number of lattice points inside B* as

$$\#(B)_T := \#(B \cap \Lambda) \qquad \text{and} \qquad \#(B)_{T,j} := \#\big(\Phi^j B\big)_T.$$

For the cell covering of a set B an alternative, perhaps more intuitive description can be given by

$$\lceil B \rceil_T := \bigcup_{\substack{z \in \Lambda \\ T_z \cap B \ne \emptyset}} T_z.$$

The following proposition deals with some basic properties that will be helpful when working with those operators.

Proposition 8.2 (Basic Properties of Cell Rounding Operations). *Let $B \subseteq \mathbb{R}^n$ and $j \in \mathbb{Z}$.*
(a) We have the inclusions

$$\lfloor B \rfloor_{T,j} \subseteq B \subseteq \overline{B} \subseteq \lceil B \rceil_{T,j}$$

and

$$\lfloor B \rfloor_{T,j} \subseteq \lfloor B \rceil_{T,j} \subseteq \lceil B \rceil_{T,j}.$$

For $B' \subseteq \mathbb{R}^n$ with $B \subseteq B'$ we get $\lfloor B \rfloor_{T,j} \subseteq \lfloor B' \rfloor_{T,j}$, $\lfloor B \rceil_{T,j} \subseteq \lfloor B' \rceil_{T,j}$ and $\lceil B \rceil_{T,j} \subseteq \lceil B' \rceil_{T,j}$, i.e., monotonicity with respect to inclusion.

(b) The inclusion

$$\{B\}_{T,j} \subseteq \partial(B)_{T,j}$$

holds.

(c) We have $\partial B \subseteq \partial(B)_{T,j}$ and for each cell T' in $\partial(B)_{T,j}$ we have $T' \cap \partial B \neq \emptyset$.

(d) For $B' \subseteq \mathbb{R}^n$ with B' disjoint from B, we get

$$\#(B \cup B')_{T,j} = \#(B)_{T,j} + \#(B')_{T,j},$$

and therefore the number of lattice points operation is monotonic with respect to inclusion, i.e., for $B'' \subseteq \mathbb{R}^n$ with $B'' \subseteq B$ we have $\#(B'')_{T,j} \leq \#(B)_{T,j}$. Further we get

$$\#(B)_{T,j} = \#\left(\lfloor B \rfloor_{T,j}\right)_{T,j} = |\det \Phi|^j \frac{\lambda\left(\lfloor B \rfloor_{T,j}\right)}{d_\Lambda}$$

Proof. The proof is a straight forward generalisation of the proof for Voronoi-tilings in the quadratic case in [12]. □

We will need some more properties concerning cardinality. We want to know the number of points inside a region after using one of the operators. Especially we are interested in the asymptotic behaviour, i.e., if our region becomes scaled very large. The following proposition provides information about that.

Proposition 8.3. *Let $U \subseteq \mathbb{R}^n$ bounded, measurable, and such that*

$$\#(\partial(\Psi U)_T)_T = \mathcal{O}\left(|\det \Psi|^{\delta/n}\right)$$

for $|\det \Psi| \to \infty$ with maps $\Psi \colon \mathbb{R}^n \to \mathbb{R}^n$ and a fixed $\delta \in \mathbb{R}$ with $\delta > 0$.

(a) *We get that each of $\#(\lfloor \Psi U \rfloor_T)_T$, $\#(\lceil \Psi U \rceil_T)_T$, $\#(\lfloor \Psi U \rceil_T)_T$ and $\#(\Psi U)_T$ equals*

$$|\det \Psi| \frac{\lambda(U)}{d_\Lambda} + \mathcal{O}\left(|\det \Psi|^{\delta/n}\right).$$

In particular, let $N \in \mathbb{R}$, $N > 0$, and set $\Psi = \mathrm{diag}(N, \ldots, N)$, which we identify with N. Then we get that each one of $\#(\lfloor NU \rfloor_T)_T$, $\#(\lceil NU \rceil_T)_T$, $\#(\lfloor NU \rceil_T)_T$ and $\#(NU)_T$ equals

$$N^n \frac{\lambda(U)}{d_\Lambda} + \mathcal{O}\left(N^\delta\right).$$

(b) *Let $N \in \mathbb{R}$, $N > 0$, and set $\Psi = \mathrm{diag}(N, \ldots, N)$, which we identify with N. Then we get*

$$\#((N+1)U \setminus NU)_T = \mathcal{O}\left(N^\delta\right).$$

Proof. Again, the proof is a straight forward generalisation of the proof for Voronoi-tilings in the quadratic case in [12]. □

Note that $\delta = n - 1$ if the U is, for example, a ball or a polyhedra.

9. The Characteristic Sets

In this section we define characteristic sets for a digit at a specified position in the w-NAF expansion and prove some basic properties of them. Those will be used in the proof of Theorem 10.1.

Definition 9.1 (Characteristic Sets). *Let $\eta \in \mathcal{D}^\bullet$. For $j \in \mathbb{N}_0$ define*

$$\mathcal{W}_{\eta,j} := \left\{\mathsf{value}(\boldsymbol{\xi}) \ : \ \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.j+w} \text{ with } \xi_{-w} = \eta\right\}.$$

We call $\lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w}$ the *jth approximation of the characteristic set for η*, and we define

$$W_{\eta,j} := \left\{\lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w}\right\}_\Lambda.$$
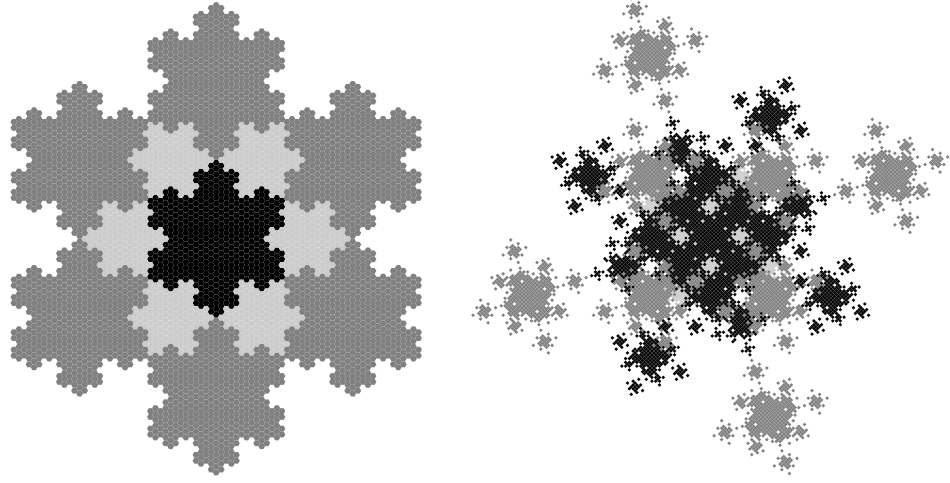
(a) $\mathcal{W}_{\eta,j}$ for a lattice coming from τ with $\tau^2 - 3\tau + 3 = 0$, $w = 2$ and $j = 7$

(b) $\mathcal{W}_{\eta,j}$ for a lattice coming from τ with $\tau^2 - 2\tau + 2 = 0$, $w = 4$ and $j = 11$

FIGURE 9.1. Fundamental domains and characteristic sets $\mathcal{W}_\eta$. Each figure shows a fundamental domain. The light-gray coloured parts represent the approximations $\mathcal{W}_{\eta,j}$ of the characteristic sets $\mathcal{W}_\eta$.

Further we define the *characteristic set for η*

$$\mathcal{W}_\eta := \big\{ \mathsf{value}(\boldsymbol{\xi}) \ : \ \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty} \text{ with } \xi_{-w} = \eta \big\}$$

and

$$W_\eta := \{\mathcal{W}_\eta\}_\Lambda \, .$$

For $j \in \mathbb{N}_0$ we set

$$\beta_{\eta,j} := \lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w} \Big) - \lambda(\mathcal{W}_\eta) \, .$$

Note that sometimes the set W_η will also be called *characteristic set for η*, and analogously for the set $W_{\eta,j}$. In Figure 9.1 some of these characteristic sets, more precisely some approximations of the characteristic sets, are shown.

The following proposition deals with some properties of those defined sets.

Proposition 9.2 (Properties of the Characteristic Sets)**.** *Let $\eta \in \mathcal{D}^\bullet$.*
(a) *We have*
$$\mathcal{W}_\eta = \eta\tau^{-w} + \Phi^{-2w+1}\mathcal{F}.$$
(b) *The set $\mathcal{W}_\eta$ is compact.*
(c) *We get*
$$\mathcal{W}_\eta = \overline{\bigcup_{j \in \mathbb{N}_0} \mathcal{W}_{\eta,j}} = \overline{\lim_{j \to \infty} \mathcal{W}_{\eta,j}}.$$
(d) *The set $\lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w}$ is indeed an approximation of $\mathcal{W}_\eta$, i.e., we have*
$$\mathcal{W}_\eta = \overline{\liminf_{j \in \mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w}} = \overline{\limsup_{j \in \mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w}}.$$
(e) *We have* $\operatorname{int} \mathcal{W}_\eta \subseteq \liminf_{j \in \mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w}$.
(f) *We get $\mathcal{W}_\eta - \Phi^{-w}\eta \subseteq T$, and for $j \in \mathbb{N}_0$ we obtain $\lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w} - \Phi^{-w}\eta \subseteq T$.*
(g) *For the Lebesgue measure of the characteristic set we obtain $\lambda(\mathcal{W}_\eta) = \lambda(W_\eta)$ and for its approximation $\lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rfloor_{T,j+w} \Big) = \lambda(W_{\eta,j})$.*

(h) Let $j \in \mathbb{N}_0$, then

$$\lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{T,j+w}\Big) = d_\Lambda E + \mathcal{O}\big(\mu^j\big)$$

with E and $\mu < 1$ from Theorem 4.7 on page 6.

(i) The Lebesgue measure of W_η is

$$\lambda(W_\eta) = d_\Lambda E,$$

again with E from Theorem 4.7 on page 6.

(j) Let $j \in \mathbb{N}_0$. We get

$$\beta_{\eta,j} = \int_{x \in T} \big(\mathbb{1}_{W_{\eta,j}} - \mathbb{1}_{W_\eta}\big)(x)\,\mathrm{d}x = \mathcal{O}\big(\mu^j\big).$$

Again $\mu < 1$ can be found in Theorem 4.7 on page 6.

Proof. The proof is a straight forward generalisation of the proof in [12]. $\qquad\square$

We can also determine the Lebesgue measure of the fundamental domain $\mathcal{F}$ defined in Section 7.

Remark 9.3 (Lebesgue Measure of the Fundamental Domain). We get

$$\lambda(\mathcal{F}) = \rho^{n(2w-1)} E d_\Lambda = \frac{\rho^{nw} d_\Lambda}{(\rho^n - 1)w + 1},$$

using (a) and (i) from Proposition 9.2 on the facing page and E from Theorem 4.7 on page 6.

The next lemma makes the connection between the w-NAFs of elements of the lattice Λ and the characteristic sets $W_{\eta,j}$.

Lemma 9.4. *Let $\eta \in \mathcal{D}^\bullet$, $j \geq 0$. Let $z \in \Lambda$ and let $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathrm{fin}.0}$ be its w-NAF. Then the following statements are equivalent:*

(1) The jth digit of $\boldsymbol{\xi}$ equals η.
(2) The condition $\big\{\Phi^{-(j+w)}z\big\}_\Lambda \in W_{\eta,j}$ holds.
(3) The inclusion $\big\{\Phi^{-(j+w)}T_z\big\}_\Lambda \subseteq W_{\eta,j}$ holds.

Proof. The proof is a straight forward generalisation of the proof of the quadratic case in [12]. $\qquad\square$

10. Counting the Occurrences of a non-zero Digit in a Region

In this section we will prove our main result on the asymptototic number of occurrences of a digit in a given region.

Note that Iverson's notation $[expr] = 1$ if $expr$ is true and $[expr] = 0$ otherwise, cf. Graham, Knuth and Patashnik [11], will be used.

Theorem 10.1 (Counting Theorem). *Let $0 \neq \eta \in \mathcal{D}$ and $N \in \mathbb{R}$ with $N > 0$. Further let $U \subseteq \mathbb{R}^n$ be measurable with respect to the Lebesgue measure and bounded with $U \subseteq \mathcal{B}(0,d)$ for a finite d, and set δ such that $\#(\partial(NU)_T)_T = \mathcal{O}\big(N^\delta\big)$ with $1 \leq \delta < n$. We denote the number of occurrences of the digit η in all integer width-w non-adjacent forms with value in the region NU by*

$$Z_\eta(N) = \sum_{z \in NU \cap \Lambda} \sum_{j \in \mathbb{N}_0} [j\text{th digit of } z \text{ in its } w\text{-NAF-expansion equals } \eta].$$

Then we get

$$Z_\eta(N) = N^n\,\lambda(U)\,E \log_\rho N + N^n\,\psi_\eta\big(\log_\rho N\big) + \mathcal{O}\big(N^\alpha \log_\rho N\big) + \mathcal{O}\big(N^\delta \log_\rho N\big),$$

in which the expressions described below are used. The Lebesgue measure on $\mathbb{R}^n$ is denoted by λ. We have the constant of the expectation

$$E = \frac{1}{\rho^{n(w-1)}((\rho^n - 1)w + 1)},$$

cf. Theorem 4.7 on page 6. Then there is the function

$$\psi_\eta(x) = \psi_{\eta,\mathcal{M}}(x) + \psi_{\eta,\mathcal{P}}(x) + \psi_{\eta,\mathcal{Q}}(x),$$

where

$$\psi_{\eta,\mathcal{M}}(x) = \lambda(U)\,(J_0 + 1 - \{x\})\,E,$$

$$\psi_{\eta,\mathcal{P}}(x) = \frac{\rho^{n(J_0 - \{x\})}}{d_\Lambda} \sum_{j=0}^{\infty} \int_{y \in \left\{\Phi^{-\lfloor x \rfloor - J_0}\rho^x U\right\}_{T,j-w}} \left(\mathbb{1}_W\left(\left\{\Phi^{j-w}y\right\}_\Lambda\right) - \lambda(W)\right) \mathrm{d}y,$$

and

$$\psi_{\eta,\mathcal{Q}} = \frac{\lambda(U)}{d_\Lambda^2} \sum_{j=0}^{\infty} \beta_j.$$

We have $\alpha = n + \log_\rho \mu < n$, with $\mu = \left(1 + \frac{1}{\rho^n w^3}\right)^{-1} < 1$, and

$$J_0 = \left\lfloor \log_\rho d - \log_\rho B_L \right\rfloor + 1$$

with the constant B_L of Proposition 5.2 on page 8.
   Further, let

$$\Phi = Q \operatorname{diag}\left(\rho e^{i\theta_1}, \ldots, \rho e^{i\theta_n}\right) Q^{-1},$$

where Q is a regular matrix. If there is a $p \in \mathbb{N}$ such that

$$Q \operatorname{diag}\left(e^{i\theta_1 p}, \ldots, e^{i\theta_n p}\right) Q^{-1} U = U,$$

then ψ_η is p-periodic. Moreover, if ψ_η is p-periodic for some $p \in \mathbb{N}$, then it is also continuous.

Remark 10.2. Consider the main term of our result. When N tends to infinity, we get the asymptotic formula

$$Z_\eta \sim N^n\,\lambda(U)\,E \log_\rho N.$$

This result is not surprising, since intuitively the number of lattice points in the region NU corresponds to the Lebesgue measure $N^n\,\lambda(U)$ of this region, and each of that elements can be represented as an integer w-NAF with length about $\log_\rho N$. Therefore, using the expectation of Theorem 4.7 on page 6, we get an explanation for this term.

Remark 10.3. If $\delta = n$ in the theorem, then the statement stays true, but degenerates to

$$Z_\eta(N) = \mathcal{O}\left(N^n \log_{|\tau|} N\right).$$

This is a trivial result of Remark 10.2.

   The proof of Theorem 10.1 on the preceding page follows the ideas used by Delange [6]. By Remark 10.3 we restrict ourselves to the case $\delta < n$.
   We will use the following abbreviations. We omit the index η, i.e., we set $Z(N) := Z_\eta(N)$, $W := W_\eta$ and $W_j := W_{\eta,j}$, and further we set $\beta_j := \beta_{\eta,j}$, cf. Proposition 9.2 on page 16. By log we will denote the logarithm to the base ρ, i.e., $\log x = \log_\rho x$. These abbreviations will be used throughout the remaining section.

Proof of Theorem 10.1. By assumption every element of Λ is represented by a unique element of $\mathbf{NAF}_w^{\text{fin},0}$. To count the occurrences of the digit η in NU, we sum up 1 over all lattice points $z \in NU \cap \Lambda$ and for each z over all digits in the corresponding w-NAF equal to η. Thus we get

$$Z(N) = \sum_{z \in NU \cap \Lambda} \sum_{j \in \mathbb{N}_0} [j\text{th digit of } w\text{-NAF of } z \text{ equals } \eta].$$

The inner sum over $j \in \mathbb{N}_0$ is finite, we will choose a large enough upper bound J later in Lemma 10.4 on the next page.

Using

$$[j\text{th digit of } w\text{-NAF of } z \text{ equals } \eta] = \mathbb{1}_{W_j}\left(\left\{\Phi^{-j-w} z\right\}_\Lambda\right)$$

from Lemma 9.4 on page 17 yields

$$Z(N) = \sum_{j=0}^{J} \sum_{z \in NU \cap \Lambda} \mathbb{1}_{W_j}\left(\left\{\Phi^{-j-w} z\right\}_\Lambda\right),$$

where additionally the order of summation was changed. This enables us to rewrite the sum over z as an integral

$$Z(N) = \sum_{j=0}^{J} \sum_{z \in NU \cap \Lambda} \frac{1}{\lambda(T_z)} \int_{x \in T_z} \mathbb{1}_{W_j}\left(\left\{\Phi^{-j-w} x\right\}_\Lambda\right) \mathrm{d}x$$

$$= \frac{1}{\lambda(T)} \sum_{j=0}^{J} \int_{x \in \lfloor NU \rceil_T} \mathbb{1}_{W_j}\left(\left\{\Phi^{-j-w} x\right\}_\Lambda\right) \mathrm{d}x.$$

We split up the integrals into the ones over NU and others over the remaining region and get

$$Z(N) = \frac{1}{\lambda(T)} \sum_{j=0}^{J} \int_{x \in NU} \mathbb{1}_{W_j}\left(\left\{\Phi^{-j-w} x\right\}_\Lambda\right) \mathrm{d}x + \mathcal{F}_\eta(N),$$

in which $\mathcal{F}_\eta(N)$ contains all integrals (with appropriate signs) over regions $\lfloor NU \rceil_T \setminus NU$ and $NU \setminus \lfloor NU \rceil_T$.

By substituting $x = \Phi^J y$, $\mathrm{d}x = |\det \Phi|^J \mathrm{d}y = \rho^{nJ} \mathrm{d}y$ we obtain

$$Z(N) = \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^{J} \int_{y \in \Phi^{-J} NU} \mathbb{1}_{W_j}\left(\left\{\Phi^{J-j-w} y\right\}_\Lambda\right) \mathrm{d}y + \mathcal{F}_\eta(N).$$

Reversing the order of summation yields

$$Z(N) = \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^{J} \int_{y \in \Phi^{-J} NU} \mathbb{1}_{W_{J-j}}\left(\left\{\Phi^{j-w} y\right\}_\Lambda\right) \mathrm{d}y + \mathcal{F}_\eta(N).$$

We rewrite this as

$$Z(N) = \frac{\rho^{nJ}}{\lambda(T)} (J+1) \lambda(W) \int_{y \in \Phi^{-J} NU} \mathrm{d}y$$

$$+ \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^{J} \int_{y \in \Phi^{-J} NU} \left(\mathbb{1}_{W}\left(\left\{\Phi^{j-w} y\right\}_\Lambda\right) - \lambda(W)\right) \mathrm{d}y$$

$$+ \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^{J} \int_{y \in \Phi^{-J} NU} \left(\mathbb{1}_{W_{J-j}}\left(\left\{\Phi^{j-w} y\right\}_\Lambda\right) - \mathbb{1}_{W}\left(\left\{\Phi^{j-w} y\right\}_\Lambda\right)\right) \mathrm{d}y$$

$$+ \mathcal{F}_\eta(N).$$

With $\Phi^{-J}NU = \lfloor\Phi^{-J}NU\rfloor_{T,j-w} \cup \{\Phi^{-J}NU\}_{T,j-w}$ for each area of integration we get

$$Z(N) = \mathcal{M}_\eta(N) + \mathcal{Z}_\eta(N) + \mathcal{P}_\eta(N) + \mathcal{Q}_\eta(N) + \mathcal{S}_\eta(N) + \mathcal{F}_\eta(N),$$

in which $\mathcal{M}_\eta$ is *"The Main Part"*, see Lemma 10.6 on the next page,

$$\mathcal{M}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)}(J+1)\,\lambda(W)\int_{y\in\Phi^{-J}NU}\mathrm{d}y, \tag{10.1a}$$

$\mathcal{Z}_\eta$ is *"The Zero Part"*, see Lemma 10.7 on the facing page,

$$\mathcal{Z}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)}\sum_{j=0}^{J}\int_{y\in\lfloor\Phi^{-J}NU\rfloor_{T,j-w}}\left(\mathbb{1}_W\big(\{\Phi^{j-w}y\}_\Lambda\big) - \lambda(W)\right)\mathrm{d}y, \tag{10.1b}$$

$\mathcal{P}_\eta$ is *"The Periodic Part"*, see Lemma 10.8 on page 22,

$$\mathcal{P}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)}\sum_{j=0}^{J}\int_{y\in\{\Phi^{-J}NU\}_{T,j-w}}\left(\mathbb{1}_W\big(\{\Phi^{j-w}y\}_\Lambda\big) - \lambda(W)\right)\mathrm{d}y, \tag{10.1c}$$

$\mathcal{Q}_\eta$ is *"The Other Part"*, see Lemma 10.9 on page 23,

$$\mathcal{Q}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)}\sum_{j=0}^{J}\int_{y\in\lfloor\Phi^{-J}NU\rfloor_{T,j-w}}\left(\mathbb{1}_{W_{J-j}} - \mathbb{1}_W\right)\big(\{\Phi^{j-w}y\}_\Lambda\big)\,\mathrm{d}y, \tag{10.1d}$$

$\mathcal{S}_\eta$ is *"The Small Part"*, see Lemma 10.10 on page 24,

$$\mathcal{S}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)}\sum_{j=0}^{J}\int_{y\in\{\Phi^{-J}NU\}_{T,j-w}}\left(\mathbb{1}_{W_{J-j}} - \mathbb{1}_W\right)\big(\{\Phi^{j-w}y\}_\Lambda\big)\,\mathrm{d}y \tag{10.1e}$$

and $\mathcal{F}_\eta$ is *"The Fractional Cells Part"*, see Lemma 10.11 on page 25,

$$\begin{aligned}
\mathcal{F}_\eta(N) = {}&\frac{1}{\lambda(T)}\sum_{j=0}^{J}\int_{x\in\lfloor NU\rfloor_T\setminus NU}\mathbb{1}_{W_j}\big(\{\Phi^{-j-w}x\}_\Lambda\big)\,\mathrm{d}x \\
&-\frac{1}{\lambda(T)}\sum_{j=0}^{J}\int_{x\in NU\setminus\lfloor NU\rfloor_T}\mathbb{1}_{W_j}\big(\{\Phi^{-j-w}x\}_\Lambda\big)\,\mathrm{d}x.
\end{aligned} \tag{10.1f}$$

To complete the proof we have to deal with the choice of J, see Lemma 10.4, as well as with each of the parts in (10.1), see Lemmata 10.6 to 10.11 on pages 21–25. The continuity of ψ_η is checked in Lemma 10.12 on page 26. $\qquad\square$

Lemma 10.4 (Choosing J). *Let $N \in \mathbb{R}_{\geq 0}$. Then every w-NAF of $\mathbf{NAF}_w^{\mathsf{fin}.0}$ with value in NU has at most $J + 1$ digits, where*

$$J = \lfloor\log N\rfloor + J_0$$

with

$$J_0 = \lfloor\log d - \log B_L\rfloor + 1$$

with B_L of Proposition 5.2 on page 8.

Proof. Let $z \in NU$, $z \neq 0$, with its corresponding w-NAF $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.0}$, and let $j \in \mathbb{N}_0$ be the largest index such that the digit ξ_j is non-zero. By using Corollary 5.3 on page 8, we conclude that

$$\rho^j B_L \leq \|z\| < Nd.$$

This means

$$j < \log N + \log d - \log B_L,$$

and thus we have

$$j \leq \lfloor\log N + \log d - \log B_L\rfloor \leq \lfloor\log N\rfloor + \lfloor\log d - \log B_L\rfloor + 1.$$

Defining the right hand side of this inequality as J finishes the proof. $\qquad\square$

Remark 10.5. For the parameter used in the region of integration in the proof of Theorem 10.1 on page 17 we get

$$\left|\det\left(\Phi^{-J}N\right)\right| = \mathcal{O}(1).$$

In particular, we get $\left\|\Phi^{-J}N\right\| = \mathcal{O}(1)$.

Proof. We have

$$\left|\det\left(\Phi^{-J}N\right)\right| = \left(\rho^{-J}N\right)^n.$$

With J of Lemma 10.4 on the facing page we obtain

$$\rho^{-J}N = \rho^{-\lfloor\log N\rfloor - J_0}\rho^{\log N} = \rho^{\log N - \lfloor\log N\rfloor - J_0} = \rho^{\{\log N\} - J_0}.$$

Since $\rho^{\{\log N\} - J_0}$ is bounded by ρ^{1-J_0}, it is $\mathcal{O}(1)$. Therefore $\det\left(\Phi^{-J}N\right)$ is $\mathcal{O}(1)$. Since $\left\|\Phi^{-1}\right\| = \rho^{-1}$ we conclude that $\left\|\Phi^{-J}N\right\|$ is $\mathcal{O}(1)$. $\qquad\square$

Lemma 10.6 (The Main Part). *For* (10.1a) *in the proof of Theorem 10.1 on page 17 we get*

$$\mathcal{M}_\eta(N) = N^n\,\lambda(U)\,E\log N + N^n\,\psi_{\eta,\mathcal{M}}(\log N)$$

with a 1-periodic function $\psi_{\eta,\mathcal{M}}$,

$$\psi_{\eta,\mathcal{M}}(x) = \lambda(U)\,(J_0 + 1 - \{x\})\,E$$

and E of Theorem 4.7 on page 6.

Proof. We have

$$\mathcal{M}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)}(J+1)\,\lambda(W)\int_{y\in\Phi^{-J}NU}\mathrm{d}y.$$

As $\lambda\left(\Phi^{-J}NU\right) = \rho^{-nJ}N^n\,\lambda(U)$ we obtain

$$\mathcal{M}_\eta(N) = \frac{\lambda(W)}{\lambda(T)}(J+1)N^n\,\lambda(U).$$

By taking $\lambda(W) = \lambda(T)\,E$ from (i) of Proposition 9.2 on page 16 and J from Lemma 10.4 on the facing page we get

$$\mathcal{M}_\eta(N) = N^n\,\lambda(U)\,E\,(\lfloor\log N\rfloor + J_0 + 1).$$

Finally, the desired result follows by using $\lfloor x\rfloor = x - \{x\}$. $\qquad\square$

Lemma 10.7 (The Zero Part). *For* (10.1b) *in the proof of Theorem 10.1 on page 17 we get*

$$\mathcal{Z}_\eta(N) = 0.$$

Proof. Consider the integral

$$I_j := \int_{y\in\lfloor\Phi^{-J}NU\rfloor_{T,j-w}}\left(\mathbb{1}_W\!\left(\left\{\Phi^{j-w}y\right\}_\Lambda\right) - \lambda(W)\right)\mathrm{d}y.$$

We can rewrite the region of integration as

$$\left\lfloor\Phi^{-J}NU\right\rfloor_{T,j-w} = \Phi^{-(j-w)}\left\lfloor\Phi^{j-w}\Phi^{-J}NU\right\rfloor_T = \Phi^{-(j-w)}\bigcup_{z\in R_{j-w}}T_z$$

for some appropriate $R_{j-w}\subseteq\Lambda$. Substituting $x = \Phi^{j-w}y$, $\mathrm{d}x = \rho^{n(j-w)}\,\mathrm{d}y$ yields

$$I_j = \rho^{-n(j-w)}\int_{x\in\bigcup_{z\in R_{j-w}}T_z}\left(\mathbb{1}_W(\{x\}_\Lambda) - \lambda(W)\right)\mathrm{d}x.$$

We split up the integral and eliminate the fractional part $\{x\}_\Lambda$ by translation to get

$$I_j = \rho^{-n(j-w)} \sum_{z \in R_{j-w}} \underbrace{\int_{x \in T} \left(\mathbb{1}_W(x) - \lambda(W) \right) \mathrm{d}x}_{=0}.$$

Thus, for all $j \in \mathbb{N}_0$ we obtain $I_j = 0$, and therefore $\mathcal{Z}_\eta(N) = 0$. $\qquad\square$

Lemma 10.8 (The Periodic Part). *For* (10.1c) *in the proof of Theorem 10.1 on page 17 we get*

$$\mathcal{P}_\eta(N) = N^n \, \psi_{\eta,\mathcal{P}}(\log N) + \mathcal{O}\left(N^\delta\right)$$

with a function $\psi_{\eta,\mathcal{P}}$,

$$\psi_{\eta,\mathcal{P}}(x) = \frac{\rho^{n(J_0 - \{x\})}}{\lambda(T)} \sum_{j=0}^{\infty} \int_{y \in \left\{ \Phi^{-\lfloor x \rfloor - J_0} \rho^x U \right\}_{T,j-w}} \left(\mathbb{1}_W\left(\left\{ \Phi^{j-w} y \right\}_\Lambda \right) - \lambda(W) \right) \mathrm{d}y.$$

Let

$$\Phi = Q \operatorname{diag}\left(\rho e^{i\theta_1}, \ldots, \rho e^{i\theta_n} \right) Q^{-1},$$

where Q *is a regular matrix. If there is a* $p \in \mathbb{N}$ *such that*

$$Q \operatorname{diag}\left(e^{i\theta_1 p}, \ldots, e^{i\theta_n p} \right) Q^{-1} U = U, \tag{10.2}$$

then $\psi_{\eta,\mathcal{P}}$ *is* p*-periodic.*

Proof. Consider

$$I_j := \int_{y \in \left\{ \Phi^{-J} N U \right\}_{T,j-w}} \left(\mathbb{1}_W\left(\left\{ \Phi^{j-w} y \right\}_\Lambda \right) - \lambda(W) \right) \mathrm{d}y.$$

The region of integration satisfies

$$\left\{ \Phi^{-J} N U \right\}_{T,j-w} \subseteq \partial\left(\Phi^{-J} N U \right)_{T,j-w} = \Phi^{-(j-w)} \bigcup_{z \in R_{j-w}} T_z \tag{10.3}$$

for some appropriate $R_{j-w} \subseteq \Lambda$.

We use the triangle inequality and substitute $x = \Phi^{j-w} y$, $\mathrm{d}x = \rho^{n(j-w)} \, \mathrm{d}y$ in the integral to get

$$|I_j| \leq \rho^{-n(j-w)} \int_{x \in \bigcup_{z \in R_{j-w}} T_z} \underbrace{\left| \mathbb{1}_W(\{x\}_\Lambda) - \lambda(W) \right|}_{\leq 1 + \lambda(W)} \mathrm{d}x.$$

After splitting up the integral and using translation to eliminate the fractional part, we get

$$|I_j| \leq \rho^{-n(j-w)} \left(1 + \lambda(W) \right) \sum_{z \in R_{j-w}} \int_{x \in T} \mathrm{d}x = \rho^{-n(j-w)} \left(1 + \lambda(W) \right) \lambda(T) \, \#(R_{j-w}).$$

Using $\#(\partial(\Psi U)_T)_T = \mathcal{O}\left(|\det \Psi|^{\delta/n} \right)$ as assumed and (10.3) we gain

$$\#(R_{j-w}) = \left| \det\left(\Phi^{-J} N \Phi^{j-w} \right) \right|^{\delta/n} = \mathcal{O}\left(\rho^{(j-w)\delta} \right),$$

because $\left| \det\left(\Phi^{-J} N \right) \right| = \mathcal{O}(1)$, see Remark 10.5 on the previous page, and $|\det \Phi| = \rho^n$. Thus

$$|I_j| = \mathcal{O}\left(\rho^{\delta(j-w) - n(j-w)} \right) = \mathcal{O}\left(\rho^{(\delta-n)j} \right).$$

Now we want to make the summation in $\mathcal{P}_\eta$ independent from J, so we consider

$$I := \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=J+1}^{\infty} I_j$$

Again we use triangle inequality and we calculate the sum to obtain

$$|I| = \mathcal{O}\big(\rho^{nJ}\big) \sum_{j=J+1}^{\infty} \mathcal{O}\big(\rho^{(\delta-n)j}\big) = \mathcal{O}\big(\rho^{nJ}\rho^{(\delta-n)J}\big) = \mathcal{O}\big(\rho^{\delta J}\big).$$

Note that $\mathcal{O}\big(\rho^{J}\big) = \mathcal{O}(N)$, so we obtain $|I| = \mathcal{O}\big(N^{\delta}\big)$.

Let us look at the growth of

$$\mathcal{P}_{\eta}(N) = \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^{J} I_j.$$

We get

$$|\mathcal{P}_{\eta}(N)| = \mathcal{O}\big(\rho^{nJ}\big) \sum_{j=0}^{J} \mathcal{O}\big(\rho^{(\delta-n)j}\big) = \mathcal{O}\big(\rho^{nJ}\big) = \mathcal{O}(N^n),$$

using $\delta < n$.

Finally, inserting J from Lemma 10.4 and extending the sum to infinity, as described above, yields

$$\mathcal{P}_{\eta}(N) = \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^{J} \int_{y \in \{\Phi^{-J}NU\}_{T,j-w}} \big(\mathbb{1}_W\big(\big\{\Phi^{j-w}y\big\}_{\Lambda}\big) - \lambda(W)\big)\, \mathrm{d}y$$

$$= N^n \psi_{\eta,\mathcal{P}}(\log N) + \mathcal{O}\big(N^{\delta}\big).$$

with the desired $\psi_{\eta,\mathcal{P}}$.

Now suppose (10.2) holds. Then

$$\Phi^{-\lfloor x\rfloor-J_0}\rho^x U = \rho^x Q \operatorname{diag}\big(\rho^{-\lfloor x\rfloor-J_0}e^{-i\theta_1(\lfloor x\rfloor+J_0)}, \ldots, \rho^{-\lfloor x\rfloor-J_0}e^{-i\theta_n(\lfloor x\rfloor+J_0)}\big) Q^{-1}U$$

$$= \rho^{\{x\}-J_0} Q \operatorname{diag}\big(e^{-i\theta_1(\lfloor x\rfloor+J_0)}, \ldots, e^{-i\theta_n(\lfloor x\rfloor+J_0)}\big) Q^{-1}U.$$

Now, we can conclude that the region of integration in $\psi_{\eta,\mathcal{P}}(x)$ is p-periodic using (10.2). All other occurrences of x in $\psi_{\eta,\mathcal{P}}(x)$ are of the form $\{x\}$, i.e., 1-periodic, so period p is obtained. $\qquad\square$

Lemma 10.9 (The Other Part). *For (10.1d) in the proof of Theorem 10.1 on page 17 we get*

$$\mathcal{Q}_{\eta}(N) = N^n \psi_{\eta,\mathcal{Q}} + \mathcal{O}(N^{\alpha}\log N) + \mathcal{O}\big(N^{\delta}\big),$$

with

$$\psi_{\eta,\mathcal{Q}} = \frac{\lambda(U)}{\lambda(T)} \sum_{j=0}^{\infty} \frac{\beta_j}{\lambda(T)}$$

and $\alpha = n + \log \mu < n$, where $\mu < 1$ can be found in Theorem 4.7 on page 6.

Proof. Consider

$$I_{j,\ell} := \int_{y \in \lfloor \Phi^{-J}NU\rfloor_{T,j-w}} \big(\mathbb{1}_{W_{\eta,\ell}} - \mathbb{1}_W\big)\big(\big\{\Phi^{j-w}y\big\}_{\Lambda}\big)\, \mathrm{d}y.$$

We can rewrite the region of integration and get

$$\big\lfloor \Phi^{-J}NU\big\rfloor_{T,j-w} = \Phi^{-(j-w)}\big\lfloor \Phi^{j-w}\Phi^{-J}NU\big\rfloor_T = \Phi^{-(j-w)} \bigcup_{z \in R_{j-w}} T_z$$

for some appropriate $R_{j-w} \subseteq \Lambda$, as in the proof of Lemma 10.7 on page 21. Substituting $x = \Phi^{j-w}y$, $\mathrm{d}x = \rho^{n(j-w)}\,\mathrm{d}y$ yields

$$I_{j,\ell} = \rho^{-n(j-w)} \int_{x \in \bigcup_{z \in R_{j-w}} T_z} \big(\mathbb{1}_{W_{\eta,\ell}} - \mathbb{1}_W\big)(\{x\}_{\Lambda})\, \mathrm{d}x$$

and further

$$I_{j,\ell} = \rho^{-n(j-w)} \sum_{z \in R_{j-w}} \underbrace{\int_{x \in T} \left(\mathbb{1}_{W_{\eta,\ell}} - \mathbb{1}_W\right)(x)\,\mathrm{d}x}_{=\beta_\ell} = \rho^{-n(j-w)}\, \#(R_{j-w})\, \beta_\ell,$$

by splitting up the integral, using translation to eliminate the fractional part and taking β_ℓ according to (j) of Proposition 9.2 on page 16. From Proposition 8.3 on page 15 we obtain

$$\frac{\#(R_{j-w})}{\rho^{n(j-w)}} = \frac{\left|\det\left(\Phi^{-J}N\Phi^{j-w}\right)\right|}{\rho^{n(j-w)}} \frac{\lambda(U)}{\lambda(T)} + \mathcal{O}\left(\frac{\left|\det\left(\Phi^{-J}N\Phi^{j-w}\right)\right|^{\delta/n}}{\rho^{n(j-w)}}\right),$$

which can be rewritten as

$$\frac{\#(R_{j-w})}{\rho^{n(j-w)}} = \rho^{-nJ}N^n\frac{\lambda(U)}{\lambda(T)} + \mathcal{O}\left(\rho^{(\delta-n)j}\right)$$

because $|\det\Phi| = \rho^n$ and because $\left|\tau^{-J}N\right| = \mathcal{O}(1)$, see Remark 10.5 on page 21.

Now let us have a look at

$$\mathcal{Q}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^{J} I_{j,J-j}.$$

Inserting the result above and using $\beta_\ell = \mathcal{O}(\mu^\ell)$, see (j) of Proposition 9.2 on page 16, yields

$$\mathcal{Q}_\eta(N) = N^n\frac{\lambda(U)}{(\lambda(T))^2} \sum_{j=0}^{J} \beta_{J-j} + \rho^{nJ}\sum_{j=0}^{J} \mathcal{O}\left(\rho^{(\delta-n)j}\right)\mathcal{O}\left(\mu^{J-j}\right).$$

Therefore, after reversing the order of the first summation, we obtain

$$\mathcal{Q}_\eta(N) = N^n\frac{\lambda(U)}{(\lambda(T))^2} \sum_{j=0}^{J} \beta_j + \rho^{nJ}\mu^J\sum_{j=0}^{J} \mathcal{O}\left(\left(\mu\rho^{n-\delta}\right)^{-j}\right).$$

If $\mu\rho^{n-\delta} \geq 1$, then the second sum is $J\,\mathcal{O}(1)$, otherwise the sum is $\mathcal{O}\left(\mu^{-J}\rho^{(\delta-2)J}\right)$. So we obtain

$$\mathcal{Q}_\eta(N) = N^n\frac{\lambda(U)}{(\lambda(T))^2} \sum_{j=0}^{J} \beta_j + \mathcal{O}\left(\rho^{nJ}\mu^J J\right) + \mathcal{O}\left(\rho^{\delta J}\right).$$

Using $J = \Theta(\log N)$, see Lemma 10.4 on page 20, and defining $\alpha = n + \log\mu$ yields

$$\mathcal{Q}_\eta(N) = N^n\frac{\lambda(U)}{(\lambda(T))^2} \sum_{j=0}^{J} \beta_j + \underbrace{\mathcal{O}\left(N^{n+\log\mu}\log N\right)}_{=\mathcal{O}(N^\alpha \log N)} + \mathcal{O}\left(N^\delta\right).$$

Now consider the first sum. Since $\beta_j = \mathcal{O}(\mu^j)$, see (j) of Proposition 9.2 on page 16, we obtain

$$N^n \sum_{j=J+1}^{\infty} \beta_j = N^n\,\mathcal{O}(\mu^J) = \mathcal{O}(N^\alpha).$$

Thus the lemma is proved, because we can extend the sum to infinity. $\square$

Lemma 10.10 (The Small Part). *For* (10.1e) *in the proof of Theorem 10.1 on page 17 we get*

$$\mathcal{S}_\eta(N) = \mathcal{O}(N^\alpha \log N) + \mathcal{O}\left(N^\delta\right)$$

with $\alpha = n + \log\mu < n$ and $\mu < 1$ from Theorem 4.7 on page 6.

Proof. Consider

$$I_{j,\ell} := \int_{y\in\{\Phi^{-J}NU\}_{T,j-w}} (\mathbb{1}_{W_\ell} - \mathbb{1}_W)\big(\big\{\Phi^{j-w}y\big\}_\Lambda\big)\,\mathrm{d}y.$$

Again, as in the proof of Lemma 10.8 on page 22, the region of integration satisfies

$$\big\{\Phi^{-J}NU\big\}_{T,j-w} \subseteq \partial\big(\Phi^{-J}NU\big)_{T,j-w} = \Phi^{-(j-w)}\bigcup_{z\in R_{j-w}} T_z \qquad (10.4)$$

for some appropriate $R_{j-w} \subseteq \Lambda$.

We substitute $x = \Phi^{j-w}y$, $\mathrm{d}x = \rho^{n(j-w)}\,\mathrm{d}y$ in the integral to get

$$|I_{j,\ell}| = \rho^{-n(j-w)}\left|\int_{x\in\bigcup_{z\in R_{j-w}} T_z} (\mathbb{1}_{W_\ell} - \mathbb{1}_W)(\{x\}_\Lambda)\,\mathrm{d}x\right|.$$

Again, after splitting up the integral, using translation to eliminate the fractional part and the triangle inequality, we get

$$|I_{j,\ell}| \le \rho^{-n(j-w)} \sum_{z\in R_{j-w}} \underbrace{\left|\int_{x\in T} (\mathbb{1}_{W_\ell} - \mathbb{1}_W)(x)\,\mathrm{d}x\right|}_{=|\beta_\ell|} = \rho^{-n(j-w)}\,\#(R_{j-w})\,|\beta_\ell|,$$

in which $|\beta_\ell| = \mathcal{O}(\mu^\ell)$ is known from (j) of Proposition 9.2 on page 16. Using $\#(\partial(\Psi U)_T)_T = \mathcal{O}\big(|\det\Psi|^{\delta/n}\big)$, Remark 10.5 on page 21, and (10.4) we get

$$\#(R_{j-w}) = \mathcal{O}\big(|\det\Phi^{-J}N\Phi^{j-w}|^{\delta/n}\big) = \mathcal{O}\big(\rho^{\delta(j-w)}\big),$$

because $|\det\Phi| = \rho^n$ and $|\tau^{-J}N| = \mathcal{O}(1)$. Thus

$$|I_{j,\ell}| = \mathcal{O}\big(\mu^\ell\rho^{(\delta-n)(j-w)}\big) = \mathcal{O}\big(\mu^\ell\rho^{(\delta-n)j}\big)$$

follows by assembling all together.

Now we are ready to analyse

$$\mathcal{S}_\eta(N) = \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^J I_{j,J-j}.$$

Inserting the result above yields

$$|\mathcal{S}_\eta(N)| = \frac{\rho^{nJ}}{\lambda(T)} \sum_{j=0}^J \mathcal{O}\big(\mu^{J-j}\rho^{(\delta-n)j}\big) = \frac{\mu^J\rho^{nJ}}{\lambda(T)} \sum_{j=0}^J \mathcal{O}\big((\mu\rho^{n-\delta})^{-j}\big)$$

and thus, by the same argument as in the proof of Lemma 10.9 on page 23,

$$|\mathcal{S}_\eta(N)| = \mu^J\rho^{nJ}\,\mathcal{O}\big(J + \mu^{-J}\rho^{(\delta-n)J}\big) = \mathcal{O}\big(\mu^J\rho^{nJ}J\big) + \mathcal{O}\big(\rho^{\delta J}\big).$$

Finally, by using Lemma 10.4 on page 20 we obtain

$$|\mathcal{S}_\eta(N)| = \mathcal{O}(N^\alpha\log N) + \mathcal{O}\big(N^\delta\big)$$

with $\alpha = n + \log\mu$. Since $\mu < 1$, we have $\alpha < n$. $\qquad\square$

Lemma 10.11 (The Fractional Cells Part)**.** *For* (10.1f) *in the proof of Theorem 10.1 on page 17 we get*

$$\mathcal{F}_\eta(N) = \mathcal{O}\big(N^\delta\log N\big).$$

Proof. For the regions of integration in $\mathcal{F}_\eta$ we obtain

$$NU \setminus \lfloor NU \rfloor_T \subseteq \lceil NU \rceil_T \setminus \lfloor NU \rfloor_T = \partial(NU)_T = \bigcup_{z \in R} T_z$$

and

$$\lfloor NU \rfloor_T \setminus NU \subseteq \lceil NU \rceil_T \setminus \lfloor NU \rfloor_T = \partial(NU)_T = \bigcup_{z \in R} T_z$$

for some appropriate $R \subseteq \Lambda$ using Proposition 8.2 on page 14. Thus we get

$$|\mathcal{F}_\eta(N)| \le \frac{2}{\lambda(T)} \sum_{j=0}^{J} \int_{x \in \bigcup_{z \in R} T_z} \mathbb{1}_{W_j}\left(\left\{\Phi^{-j-w}x\right\}_\Lambda\right) \mathrm{d}x \le \frac{2}{\lambda(T)} \sum_{j=0}^{J} \sum_{z \in R} \int_{x \in T_z} \mathrm{d}x,$$

in which the indicator function was replaced by 1. Dealing with the sums and the integral, which is $\mathcal{O}(1)$, we obtain

$$|\mathcal{F}_\eta(N)| = (J+1)\#R\,\mathcal{O}(1).$$

Since $J = \mathcal{O}(\log N)$, see Lemma 10.4 on page 20, and $\#R = \mathcal{O}\left(N^\delta\right)$, the desired result follows. □

Lemma 10.12. *If the ψ_η from Theorem 10.1 on page 17 is p-periodic for some $p \in \mathbb{N}$, then ψ_η is also continuous.*

Proof. There are two possible parts of ψ_η where an discontinuity could occur: the first is $\{x\}$ for an $x \in \mathbb{Z}$, the second is building $\{\ldots\}_{T,j-w}$ in the region of integration in $\psi_{\eta,\mathcal{P}}$.

The latter is no problem, i.e., no discontinuity, since

$$\int_{y \in \left\{\Phi^{-\lfloor x \rfloor - J_0} \rho^x U\right\}_{T,j-w}} \left(\mathbb{1}_W\left(\left\{\Phi^{j-w}y\right\}_\Lambda\right) - \lambda(W)\right) \mathrm{d}y$$

$$= \int_{y \in \Phi^{-\lfloor x \rfloor - J_0} \rho^x U} \left(\mathbb{1}_W\left(\left\{\Phi^{j-w}y\right\}_\Lambda\right) - \lambda(W)\right) \mathrm{d}y,$$

because the integral over the region $\left\lfloor \Phi^{-\lfloor x \rfloor - J_0} \rho^x U \right\rfloor_{T,j-w}$ is zero, see proof of Lemma 10.7 on page 21.

Now we deal with the continuity at $x \in \mathbb{Z}$. Let $m \in x + p\mathbb{Z}$, let $M = \rho^m$, and consider

$$Z_\eta(M) - Z_\eta(M-1).$$

For an appropriate $a \in \mathbb{R}$ we get

$$Z_\eta(M) = aM^n \log M + M^n \psi_\eta(\log M) + \mathcal{O}(M^\alpha \log M) + \mathcal{O}\left(M^\delta \log M\right),$$

and thus

$$Z_\eta(M) = aM^n m + M^n \underbrace{\psi_\eta(m)}_{=\psi_\eta(x)} + \mathcal{O}(M^\alpha m) + \mathcal{O}\left(M^\delta m\right).$$

Further we obtain

$$Z_\eta(M-1) = a\,(M-1)^n \log(M-1) + (M-1)^n \psi_\eta(\log(M-1))$$
$$+ \mathcal{O}((M-1)^\alpha \log(M-1)) + \mathcal{O}\left((M-1)^\delta \log(M-1)\right),$$

and thus, using the abbreviation $L = \log\left(1 - M^{-1}\right)$ and $\delta \ge 1$,

$$Z_\eta(M-1) = aM^n m + M^n \underbrace{\psi_\eta(m+L)}_{=\psi_\eta(x+L)} + \mathcal{O}(M^\alpha m) + \mathcal{O}\left(M^\delta m\right).$$

Therefore we obtain

$$\frac{Z_\eta(M) - Z_\eta(M-1)}{M^n} = \psi_\eta(x) - \psi_\eta(x+L) + \mathcal{O}\big(M^{\alpha-n}m\big) + \mathcal{O}\big(M^{\delta-n}m\big).$$

Since $\#(MU \setminus (M-1)U)_T$ is clearly an upper bound for the number of w-NAFs with values in $MU \setminus (M-1)U$ and each of these w-NAFs has at most $\lfloor \log M \rfloor + J_0 + 1$ digits, see Lemma 10.4 on page 20, we obtain

$$Z_\eta(M) - Z_\eta(M-1) \le \#(MU \setminus (M-1)U)_T \, (m + J_0 + 2).$$

Using (b) of Proposition 8.3 on page 15 yields

$$Z_\eta(M) - Z_\eta(M-1) = \mathcal{O}\big(M^\delta m\big).$$

Therefore we get

$$\psi_\eta(x) - \psi_\eta(x+L) = \mathcal{O}\big(M^{\delta-n}m\big) + \mathcal{O}\big(M^{\alpha-n}m\big) + \mathcal{O}\big(M^{\delta-n}m\big).$$

Taking the limit $m \to \infty$ in steps of p, and using $\alpha < n$ and $\delta < n$ yields

$$\psi_\eta(x) - \lim_{\varepsilon \to 0^-} \psi_\eta(x+\varepsilon) = 0,$$

i.e., ψ_η is continuous at $x \in \mathbb{Z}$. $\qquad\qquad\square$

11. Counting Digits in Conjunction with Hyperelliptic Curve Cryptography

As mentioned in the introduction, we are interested in numeral systems coming from hyperelliptic curve cryptography. There the base is an algebraic integer, where all conjugates have the same absolute value.

Let H be a hyperelliptic curve (or more generally an algebraic curve) of genus g defined over $\mathbb{F}_q$ (a field with q elements). The Frobenius endomorphism operates on the Jacobian variety of H and satisfies a characteristic polynomial $f \in \mathbb{Z}[T]$ of degree $2g$. This polynomial fulfils the equation

$$f(T) = T^{2g}L(1/T),$$

where $L(T)$ denotes the numerator of the zeta-function of H over $\mathbb{F}_q$, cf. Weil [19, 21]. The Riemann Hypothesis of the Weil Conjectures, cf. Weil [20], Dwork [8] and Deligne [7], states that all zeros of L have absolute value $1/\sqrt{q}$. Therefore all roots of f have absolute value $\sqrt{q}$.

Later we suppose that τ is a root of f, and we consider numeral systems with a base τ. But before, we describe getting from that setting to a lattice, which we need in Section 3. This is generally known and was also used in Heuberger and Krenn [14].

First consider a number field K of degree n. Denote the real embeddings of K by $\sigma_1, \ldots, \sigma_s$ and the non-real complex embeddings of K by $\sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$, where $\overline{\cdot}$ denotes complex conjugation and $n = s + 2t$. The *Minkowski map* $\Sigma \colon K \to \mathbb{R}^n$ maps $\alpha \in K$ to

$$(\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \Re\sigma_{s+1}(\alpha), \Im\sigma_{s+1}(\alpha), \ldots, \Re\sigma_{s+t}(\alpha), \Im\sigma_{s+t}(\alpha)) \in \mathbb{R}^n.$$

Now let τ be an algebraic integer of degree n (as above, where τ was supposed to be a root of the characteristic polynomial f of the Frobenius endomorphism) and such that all its conjugates have the same absolute value $\rho > 1$. Note that the absolute value of the field norm of τ equals ρ^n. Set $K = \mathbb{Q}(\tau)$ and consider the order $\mathbb{Z}[\tau]$. We get a lattice $\Lambda = \Sigma(\mathbb{Z}[\tau])$ of degree n in the space $\mathbb{R}^n$. Application of the map $\Phi \colon \Lambda \to \Lambda$ on a lattice element should correspond to the multiplication by τ in the order, so we define Φ as block diagonal matrix by

$$\Phi := \mathrm{diag}\left(\sigma_1(\tau), \ldots, \sigma_s(\tau), \begin{pmatrix} \Re\sigma_{s+1}(\tau) & -\Im\sigma_{s+1}(\tau) \\ \Im\sigma_{s+1}(\tau) & \Re\sigma_{s+1}(\tau) \end{pmatrix}, \ldots, \begin{pmatrix} \Re\sigma_{s+t}(\tau) & -\Im\sigma_{s+t}(\tau) \\ \Im\sigma_{s+t}(\tau) & \Re\sigma_{s+t}(\tau) \end{pmatrix}\right).$$

The eigenvalues of Φ are exactly the conjugates of τ, therefore all eigenvalues have absolute value ρ. For the norm $\|\cdot\|$ we choose the Euclidean norm $\|\cdot\|_2$. Then the corresponding operator norm fulfils

$$\|\Phi\| = \max\left\{|\sigma_j(\tau)| \,:\, j \in \{1, 2, \ldots, s+t\}\right\} = \rho.$$

In the same way we get $\left\|\Phi^{-1}\right\| = \rho^{-1}$.

Now let $T \subseteq \mathbb{R}^n$ be a set which tiles the $\mathbb{R}^n$ by the lattice Λ, choose w as in the set-up in Section 3, and let $\mathcal{D}$ be a reduced residue digit set modulo Φ^w corresponding to the tiling, cf. also Heuberger and Krenn [14]. Since our lattice Λ comes from the order $\mathbb{Z}[\tau]$ and our map Φ corresponds to the multiplication by τ map, the size of the digit set $\mathcal{D}$ is $\rho^{n(w-1)}\left(\rho^n - 1\right) + 1$, see [12] for details.

Since our set-up, see Section 3, is now complete, we get that Theorem 10.1 holds. We want to restate this for our special case of τ-adic w-NAF-expansions. This is done in Corollary 11.2. To prove periodicity of the function ψ_η in that corollary, we need the following lemma.

Lemma 11.1. *Suppose*

$$\Phi = Q \operatorname{diag}\left(\rho e^{i\theta_1}, \ldots, \rho e^{i\theta_n}\right) Q^{-1},$$

where Q is a regular matrix and let $U = \mathcal{B}(0, 1)$ be the unit ball. Then

$$Q \operatorname{diag}\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right) Q^{-1} U = U.$$

Proof. Since Φ is normal, the matrix $Q \operatorname{diag}\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right) Q^{-1}$ is unitary. Therefore balls are mapped to balls bijectively, which was to prove. $\qquad\square$

Now, as mentioned above, we reformulate Theorem 10.1 for our τ-adic set-up. This gives the following corollary.

Corollary 11.2. *Let τ be an algebraic integer, where all conjugates have the same absolute value, denote the embeddings of $\mathbb{Q}(\tau)$ by $\sigma_1, \ldots, \sigma_{s+t}$ as above, and define a norm by $\|z\|^2 = \sum_{i=1}^{s+t} d_i \, |\sigma_i(z)|^2$ with $d_1 = \cdots = d_s = 1$ and $d_{s+1} = \cdots = d_{s+t} = 2$.*

Let $0 \neq \eta \in \mathcal{D}$ and $N \in \mathbb{R}$ with $N > 0$. We denote the number of occurrences of the digit η in all width-w non-adjacent forms in $\mathbb{Z}[\tau]$, where the norm of its value is smaller than N, by

$$Z_\eta(N) = \sum_{\substack{z \in \mathbb{Z}[\tau] \\ \|z\| < N}} \sum_{j \in \mathbb{N}_0} \left[\text{jth digit of z in its w-NAF-expansion equals η}\right].$$

Then we get

$$Z_\eta(N) = N^n \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2} + 1\right)} E \log_\rho N + N^n \, \psi_\eta\left(\log_\rho N\right) + \mathcal{O}\left(N^\beta \log_\rho N\right),$$

where we have the constant of the expectation

$$E = \frac{1}{\rho^{n(w-1)}((\rho^n - 1)w + 1)},$$

cf. Theorem 4.7 on page 6, a function $\psi_\eta(x)$ which is 1-periodic and continuous and $\beta < n$.

Proof. We choose $U = \mathcal{B}(0, 1)$ the unit ball in the $\mathbb{R}^n$. Then U is measurable, $d = 1$ and $\delta = n - 1 < n$. Further the n-dimensional Lebesgue measure of U equals $\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}$. The condition $\#(\partial(NU)_T)_T = \mathcal{O}\left(N^\delta\right)$ can be checked easily. In the case of a quadratic τ this is done in [12]. The periodicity (and therefore continuity) of ψ_η follows from Lemma 11.1. We can choose $\beta = \max\{\alpha, n-1\}$. $\qquad\square$

References

1. Roberto M. Avanzi, Henri Cohen, Cristophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press Series on Discrete Mathematics and its Applications, vol. 34, Chapman & Hall/CRC, Boca Raton, FL, 2005. (Cited on page 1.)

2. Michael Barnsley, *Fractals everywhere*, Academic Press, Inc, 1988. (Cited on page 11.)

3. Ian F. Blake, V. Kumar Murty, and Guangwu Xu, *Efficient algorithms for Koblitz curves over fields of characteristic three*, J. Discrete Algorithms **3** (2005), no. 1, 113–124. (Cited on page 2.)

4. ———, *A note on window τ-NAF algorithm*, Inform. Process. Lett. **95** (2005), 496–502. (Cited on page 2.)

5. ———, *Nonadjacent radix-τ expansions of integers in Euclidean imaginary quadratic number fields*, Canad. J. Math. **60** (2008), no. 6, 1267–1282. (Cited on page 2.)

6. Hubert Delange, *Sur la fonction sommatoire de la fonction "somme des chiffres"*, Enseignement Math. (2) **21** (1975), 31–47. (Cited on pages 2 and 18.)

7. Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. (Cited on pages 2 and 27.)

8. Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. (Cited on pages 2 and 27.)

9. Gerald A. Edgar, *Measure, topology, and fractal geometry*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2008. (Cited on pages 4, 11, 13, and 14.)

10. Peter J. Grabner, Clemens Heuberger, and Helmut Prodinger, *Distribution results for low-weight binary representations for pairs of integers*, Theoret. Comput. Sci. **319** (2004), 307–331. (Cited on page 2.)

11. Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics. A foundation for computer science*, second ed., Addison-Wesley, 1994. (Cited on pages 7 and 17.)

12. Clemens Heuberger and Daniel Krenn, *Analysis of width-w non-adjacent forms to imaginary quadratic bases*, Tech. Report 2010-10, Graz University of Technology, 2010, available at `http://www.math.tugraz.at/fosp/pdfs/tugraz_0168.pdf`, also available at arXiv:1009.0488v2 [math.NT]. (Cited on pages 2, 3, 4, 6, 9, 10, 11, 15, 17, and 28.)

13. ———, *Optimality of the width-w non-adjacent form: General characterisation and the case of imaginary quadratic bases*, arXiv:1110.0966v1 [math.NT], 2011. (Cited on page 2.)

14. ———, *Existence and optimality of w-non-adjacent forms with an algebraic integer base*, arXiv:1205.5414v1 [math.NT], 2012. (Cited on pages 2, 5, 27, and 28.)

15. Clemens Heuberger and Helmut Prodinger, *Analysis of alternative digit sets for nonadjacent representations*, Monatsh. Math. **147** (2006), 219–248. (Cited on pages 2 and 11.)

16. Neal Koblitz, *An elliptic curve implementation of the finite field digital signature algorithm*, Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998), Lecture Notes in Comput. Sci., vol. 1462, Springer, Berlin, 1998, pp. 327–337. (Cited on page 2.)

17. Jerome A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology — CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings (B. S. Kaliski, jun., ed.), Lecture Notes in Comput. Sci., vol. 1294, Springer, Berlin, 1997, pp. 357–371. (Cited on page 2.)

18. ———, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249. (Cited on page 2.)

19. André Weil, *Variétés abéliennes et courbes algébriques*, Actualités scientifiques et industrielles, no. 1064, Hermann & Cie, 1948. (Cited on pages 2 and 27.)

20. ———, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. (Cited on pages 2 and 27.)

21. ———, *Courbes algébriques et variétés abéliennes*, Hermann, 1971. (Cited on pages 2 and 27.)

Daniel Krenn

Institute of Optimisation and Discrete Mathematics (Math B)

Graz University of Technology

Steyrergasse 30/II, A-8010 Graz, Austria

E-mail address: `math@danielkrenn.at` *or* `krenn@math.tugraz.at`